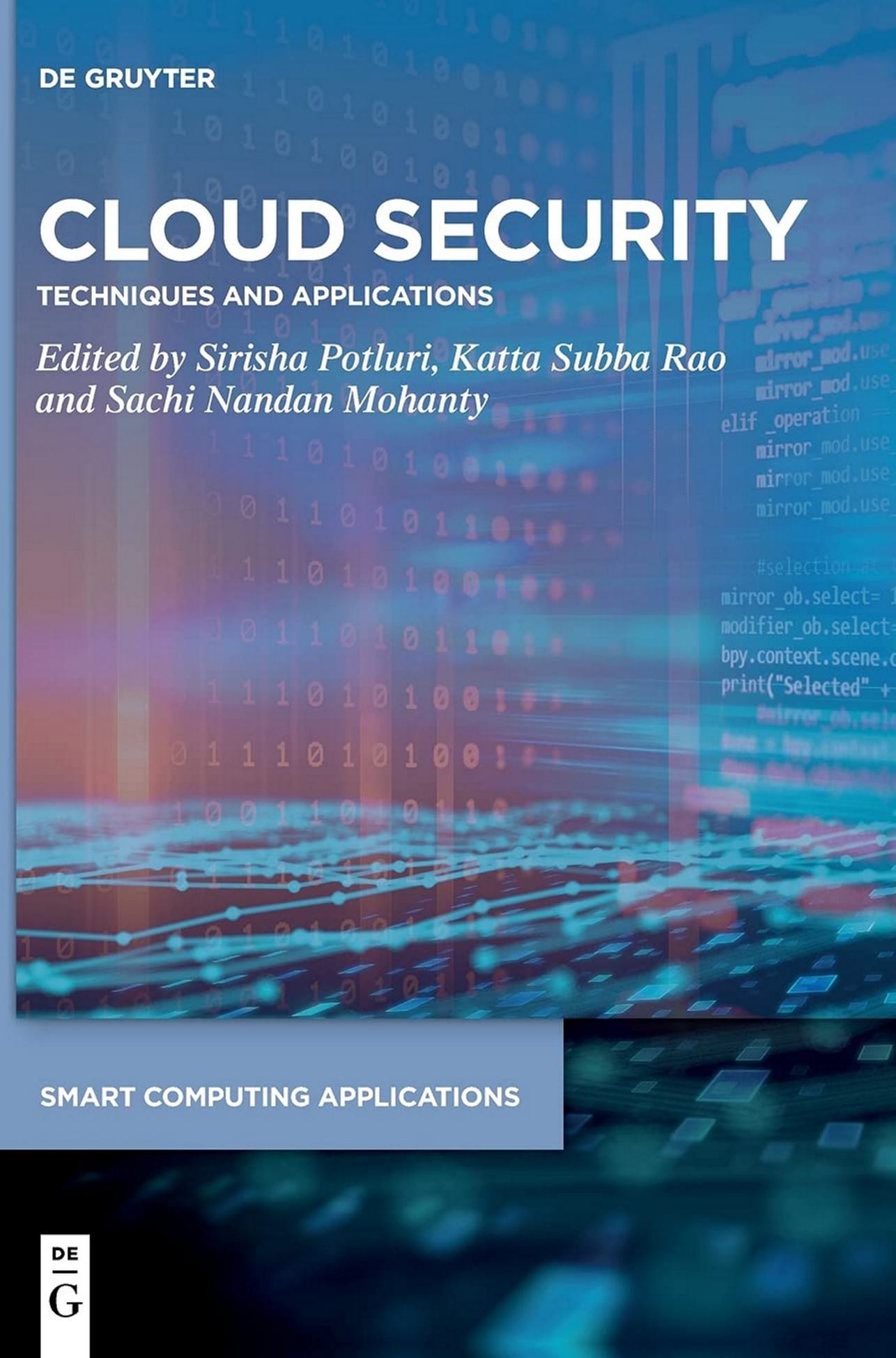
DE GRUYTER
CLOUD SECURITY
TECHNIQUES AND APPLICATIONS
Edited by Sirisha Potluri, Katta Subba Rao and Sachi Nandan Mohanty
SMART COMPUTING APPLICATIONS
DE G

Sirisha Potluri, Katta Subba Rao, Sachi Nandan Mohanty (Eds.)
Cloud Security

De Gruyter Series on Smart Computing Applications

Edited by Prasenjit Chatterjee, Dilbagh Panchal, Dragan Pamucar, Sarfaraz Hashemkhani Zolfani

Volume 1

Cloud Security

Techniques and Applications

Edited by Sirisha Potluri, Katta Subba Rao,
Sachi Nandan Mohanty

DE GRUYTER

Editors

Asst.Prof. Sirisha Potluri
ICFAI Foundation for Higher Education
Department of CSE, IcfaiTech
Faculty of Science and Technology
Donthanpally Shankarpalli Road
Telangana-501203
India
sirisha.vegunta@gmail.com

Dr. Katta Subba Rao
B.V.Raju Institute of Technology
Department of CSE
Medak District
Telangana-502313
India
subbarao.k@bvrit.ac.in

Dr. Sachi Nandan Mohanty
College of Engineering Pune
Department of Computer Engineering
Wellesley Road, Shivajinagar, Pune
Maharashtra-411005
India
sachinandan09@gmail.com

ISBN 978-3-11-073750-9
e-ISBN (PDF) 978-3-11-073257-3
e-ISBN (EPUB) 978-3-11-073270-2
ISSN 2700-6239

Library of Congress Control Number: 2021939885

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available on the Internet at http://dnb.dnb.de.

Cover image: monsitj / iStock / Getty Images Plus
Printing and binding: CPI books GmbH, Leck

www.degruyter.com

This book is humbly dedicated in honour of Shri N. J. Yasaswy, Finance and investment writer and founder of ICFAI University and Shri E. N. Murthy, Member Secretary, The ICFAI Society, whose support, encouragement and blessings made us to get this effort and work.

Aforesaid volume contains the devotion with great love and affection “In memory of my beloved father Shri Potluri. Rama Mohana Rao”, whose foundation, inspiration and benediction made me to achieve this great career and life.

Preface

Sustainable computing paradigms like cloud and fog are mining better solutions to handle the issues of security, privacy, performance, storage, processing, maintenance, efficiency, integration, cost, energy and latency. In these evolving days, according to statistics, billions of connected devices are producing enormous amounts of real time data. For complex computation and processing of the collected data in order to make the dynamic decisions these devices are connected over the cloud or fog environment. Best practices and protocols are being implemented by cloud to ensure security and privacy everywhere in the architecture.

This book illuminates some of the best practices and their respective outcomes in cloud environment to preserve privacy and security. This book is aiming to provide next level of security and privacy preserving techniques for dynamic cloud. Innovative techniques and methods for secure cloud are gathered to present advanced and specialized research in the selected area.

Various state-of-the-art and cutting edge methods to achieve security and privacy in cloud computing environment by using Artificial intelligence, Machine learning, Blockchain, IoT, DDoS mitigating practices, Industry 4.0, Cloud manufacturing, Data analytics and Vanet are essential slices of this book.

This book essences on various research issues related to security and privacy preserving approaches and techniques using big data storage and analysis, large scale data processing, knowledge discovery and knowledge management, computational intelligence, data security and privacy, data representation and visualization and data analytics. The featured technology of this book optimizes various industry processes using business intelligence in engineering and technology. This book sheds light on cloud based secure integrated and development practices to increase productivity and reduce the operational cost.

Chapter 1 focuses on AI based advanced technology that helps companies to manage complex operations efficiently and improve productivity. AI-based networks allows to maximize organizational performance but also to evade risks and threats. This chapter focuses on security and privacy related issues and explored effective counter measure to handle such issues. This chapter also provides latest literature on collaboratively secured collections to identify the kind of vulnerability they address and also the form of approach they use to handle it.

Chapter 2 focuses on Blockchain based advanced technology to deliver infrastructure and has been adopted widely due to its performance and availability. Blockchain Technology, one of the emerging technologies can be used to complement the issues concerning cloud users. This technology provides features like decentralization, distribution, authenticity, immutability, trust, etc. that can be used to face the threats of data integrity. This chapter focuses on concerning the security

https://doi.org/10.1515/9783110732573-202

and privacy of the data in the cloud model and how the features of the blockchain technology can enhance the integrity of this model.

Chapter 3 focuses on DDoS attack occurrences, DDoS types and associated security and privacy issues in cloud computing environment. Due to the dynamic behavior, distributed paradigm and heterogeneity present among the processing elements, devices and service oriented pay per use policies; the cloud computing environment is having its availability, security and privacy issues. Among these various issues one of the important issues in cloud computing paradigm is DDoS attack. This chapter put in plain words the DDoS attack, its detection as well as prevention mechanisms in cloud computing environment. This chapter also explains about the effects of DDoS attack on cloud platform and the related defence mechanisms required to be considered.

Chapter 4 focuses on secure cloud based healthcare application to handle big data of healthcare industry. Handling and processing such huge chunks of data can be a daunting task. To avoid scenarios of this type, many of the healthcare sectors have adapted cloud computing as the solution. This chapter explains privacy related issues and security related concerns, dynamically acceptable storage, regulatory issues, electronic documents containing patient's data, handwritten medical editions, various images such as X-ray, MRI scan and radiology images analysis.

Chapter 5 focuses on secure IoT frameworks, methods, security arrangements, and the best protection models are important and suitable for the various layers of IoT operated applications. This chapter also proposed embossed IoT model: standard and expanded with security and safety components and layers of physical evidence. This chapter also explains about perceived security vulnerabilities and best security measures to combat network security risks in all layers of cloud, edge, and IoT.

Chapter 6 focuses on efficient marketing strategies for business to business marketing and business to customer marketing are greatly heightened by using cloud based marketing automation solutions. Cloud governance ensure to meet business desires and needs through professional practices. Significant factors to ensure security in cloud marketing are embedded in each phase of marketing life cycle. This chapter explains about various cloud based secure marketing solutions to meet next generation marketing needs.

Chapter 7 focuses on secure machine learning model to anticipate in finest outcomes and boost the choice of cloud based long-term course of actions. This chapter is proposing best strategic cloud security enhancement model for next generation computing standards. Efficient machine learning algorithms like convolution neural network gives automatic and responsive approaches to reinforce security in a cloud environment. These models give solutions that incorporate holistic approaches for secure enterprise knowledge throughout all the cloud applications.

Chapter 8 focuses on secure intelligent VANET for smart transportation to observe resolutions using cloud based infrastructure. The vehicles connect together

through a network to form a vehicular cloud which will offer space for storing, computing resources, sensor readings as an on-demand service to clients. There is a need of efficient computational, supervising and guiding solutions for the citizens to make them to get rid of traffic related issues and problems. This chapter explains various methods to find an appropriate parking lot within the area on the brink of university, shopping complex, or a commercial complex in big and medium cities would enjoy the assistance of an automatic parking management utility.

Chapter 9 focuses on novel cloud manufacturing architype which is developed from prevailing innovative manufacturing prototypes and enterprise level information expertise under the provision of cloud computing, IoT, virtualization technology and service oriented computing, and cutting-edge computing technologies and expertise. Manufacturing as a service is an advanced manufacturing architype developed from the existing manufacturing models such as ASP, AM, NM and MGrid. This chapter is to study and discuss about security and privacy issues and solutions in cloud based manufacturing.

Sirisha Potluri, India
Katta Subba Rao, India
Sachi Nandan Mohanty, India

Acknowledgement

The editors would like to acknowledge and pass on good wishes and show appreciation to all the authors for contributing their chapters. We would also like to thank the subject matter experts who could find their time to review the chapters and deliver those in time. Our special thanks to the people who gave their time to advice and suggest in refining our thoughts and approaches accordingly to produce richer contributions. We are particularly grateful to the Walter de Gruyter GmbH publishers for their amazing crew to support us in all ways of encouragement, engagement, support, cooperation and contribution to publish this book.

https://doi.org/10.1515/9783110732573-203

Contents

List of Abbreviations

AI	Artificial Intelligence
DI	Data Integrity
DU	Data Usage
TTP	Third Party Based Encryption Scheme
VM	Virtual Machine
CDC	Centralized Data Centre
ANN	Artificial Neural Network
MSE	Mean Squared Error
DNN	Deep Neural Network
IoT	Internet of Things
CSP	Cloud Service Provider
SAMS	Secure Authentication Management human-centric Scheme
DDoS	Distributed-Denial-of-Service
DoS	Denial-of-service
SLA	Service Level Agreement
SDN	Software Defined Network
KNN	K nearest Neighbour
SOA	Service Oriented Architecture
BW-DDoS	Bandwidth distributed Dos
CDN	Content Delivery Network
SMC	Secure Multiparty Computation
API	Application Programming Interface
VMM	Virtual Machine Manager
SaaS	Software as a Service
PaaS	Platform as a Service
IaaS	Infrastructure as a Service
BDaaS	Big Data as a Service
NaaS	Network as a Service
HaaS	Healthcare as a Service
MaaS	Manufacturing as a Service
IoTaaS	IoT as a Service
AaaS	Analytics as a Service
EMS	Emergency Medical Systems
CNN	Convolutional Neural Network
AWS	Amazon Web Service
RFID	Radio Frequency Identification
IAM	Identity and Access Management
SEO	Search Engine Optimization
SEM	Search Engine Marketing

https://doi.org/10.1515/9783110732573-205

CRM	Customer Relationship Management
CapEx	Capital Expense
OpEx	Operating Expenditure
RACE	Reach, Act, Convert, and Engage
CRO	Conversion Rate Optimization
LPO	Landing Page Optimization
SMB	Small and Medium Sized Businesses
BFSI	Financial Services and Insurance
PPC	Pay-Per-Click
CTA	Call to Action
ML	Machine Learning
CAGR	Compound Annual Growth Rate
SIEM	Security Information and Event Management System
VCC	Vehicular Cloud Computing
VANET	Vehicular Ad hoc Network
LTE	Long Term Evolution
WAVE	Wireless Access Vehicular Environment
DSRC	Dedicated Short Range Communication
BSM	Basic Safety Message
QoS	Quality of Service
LIDAR	Laser Illuminated Detection and Ranging
SARTRE	Safe Road Trains for the Environment
VC	Vehicular Cloud
PKI	Public Key Infrastructure
CRL	Certificate Revocation List
CA	Certificate Authority
ITS	Intelligent Transportation Systems
ECPP	Enhanced Conditional Privacy Preservation
PACP	Pseudonymous Authentication-Based Conditional Privacy

List of Contributors

Ms. Sirisha Potluri working as Assistant Professor in the Department of Computer Science & Engineering at ICFAI Foundation for Higher Education, Hyderabad. She is pursuing her PhD in the area of cloud computing from KL Education Foundation, Vijayawada, India. Her research areas include Distributed Computing, Cloud Computing, Fog Computing, Recommender Systems and IoT. She has 7+ years of teaching experience. Her teaching subjects include Computer Programming using C, Data Structures, Core JAVA, Advanced JAVA, OOP through C++, Distributed Operating System, Human Computer Interaction, C# and .NET Programming, Computer Graphics, Web Technology, UNIX Programming, Distributed and Cloud Computing, Python Programming and Software Engineering. She has published 22 scholarly peer reviewed research articles in reputed International Journals. She has attended 11 international conferences organized by various professional bodies like IEEE and Spinger to present her novel research papers. She has a patent in cloud computing domain and edited two books. She is a member of IEEE Computer Society. Sirisha is a reviewer for various journals of Inderscience Publishers and reviewed many manuscripts.

Dr. Sachi Nandan Mohanty , Associate Professor in the Department of Computer Engineering at the College of Engineering Pune, India. He received his PostDoc from IIT Kanpur in the year 2019 and Ph.D. from IIT Kharagpur, India in the year 2015, with MHRD scholarship from Govt of India. He has edited 14 books in association with Springer, Wiley and CRC Press. His research areas include Data mining, Big Data Analysis, Cognitive Science, Fuzzy Decision Making, Brain-Computer Interface, and Computational Intelligence. Prof. S N Mohanty has received 3 Best Paper awards during his Ph.D at IIT Kharagpur from International Conference at Benjing, China, and the other at International Conference on Soft Computing applications organized by IIT Rookee in the year 2013. He has awarded Best thesis award first prize by Computer Society of India in the year 2015. He has published 42 International Journals of International repute and has been elected as FELLOW of Institute of Engineers, IETE, and senior member of IEEE Computer Society Hyderabad chapter. He also the reviewer of Journal of Robotics and Autonomous Systems (Elsevier), Computational and Structural Biotechnology Journal (Elsevier), Artificial Intelligence Review (Springer), Spatial Information Research (Springer).

Dr. Katta Subba Rao is working as a Professor in Department of Computer Science & Engineering in B.V.Raju Institute of Technology, Hyderabad, India. He has received PhD degree from Nagarjuna University, Andhra Pradesh, India. His research areas includes Software Engineering, Cloud Computing and Machine Learning. He has more than 15 years of cherished teaching and research experience. His research contributes various journal articles, conferences and book chapters.

Dr. Gouse Baig Mohammad is working as Associate Professor in Department of Computer Science & Engineering in Vardhaman College of Engineering, Hyderabad, India. He has received PhD degree from Nagarjuna University, Andhra Pradesh, India. His research areas includes Network Security, IoT and Machine Learning. He has 14 years of cherished teaching and research experience. His research contributes 7 scholarly peer reviewed research articles in reputed International Journals and 2 patents.

Mr. Srikanth Pothuri is working as National Head, Department of Marketing, at ICFAI Foundation for Higher Education, Hyderabad, India. He is pursuing his PhD from ICFAI Business School, ICFAI University Dehradun, Dehradun, Uttarakand, India. His research areas include Marketing Management,

Marketing Strategy, Consumer Behavior and Marketing Quantitative Methods. He has 19 years of industry experience.

Mr. V. MNSSVKR GUPTA is working as Assistant professor in Sagi Rama Krishnam Raju Engineering College (SRKR Engineering College), Bhimavaram, India. He is pursuing his PhD from KL Education Foundation, Vijayawada, India. His research areas include Artificial Intelligence, Bio Informatics and Image Processing. He has 12 years of teaching experience. He has published 11 scholarly peer reviewed research articles in reputed International Journals and attended 5 international conferences.

Mr. Vangeti Bhanu Prakash Reddy is a researcher in the Department of Computer Science and Engineering at ICFAI Foundation for Higher Education, IcfaiTech (Faculty of Science and Technology), Hyderabad, India. His research interest includes Artificial Intelligence, Cloud Computing and Machine Learning.

Mr. Srinath Bellamkonda is a researcher in the Department of Computer Science and Engineering at ICFAI Foundation for Higher Education, IcfaiTech (Faculty of Science and Technology), Hyderabad, India. His research interest includes Artificial Intelligence, Cloud Computing and Machine Learning.

Mr. Manjunath Reddy is a researcher in the Department of Computer Science and Engineering at ICFAI Foundation for Higher Education, IcfaiTech (Faculty of Science and Technology), Hyderabad, India. His research interest includes Artificial Intelligence, Cloud Computing and Machine Learning.

Mr. Shagun S Lokre is a researcher in the Department of Computer Science and Engineering at ICFAI Foundation for Higher Education, IcfaiTech (Faculty of Science and Technology), Hyderabad, India. His current area of interest for research includes Blockchain technology, Ethereum, Distributed Ledger Technology, Supply chain management. As a part of his achievements, he has an approved patent in the field of Blockchain technology in the event management sector in the India patent office (IPO), and co-authored 3 chapters titled “Gun Tracking System Using Blockchain Technology”, “Secure Event Ticket Booking Using Blockchain Technology”, “Distributed Ledger Technology in the Construction Industry Using Corda” in Blockchain Technology. These chapters are part of “Blockchain Technology: Applications and Challenges”, “Intelligent Systems Reference Library, Springer (WoS and Scopus Indexed)”, and “The New Advanced Society: Artificial Intelligence and Industrial Internet of Things Paradigm, Willey Press (U.S.A)”. He is currently working on other research papers on the Distributed Ledger Technology.

Ms. Shanmukhi Priya, is a researcher in the Department of Computer Science and Engineering at ICFAI Foundation for Higher Education, IcfaiTech (Faculty of Science and Technology), Hyderabad, India. Her current area of interest for research includes blockchain technology, Ethereum, Distributed Ledger technology, Corda, and back-end technologies. As a part of his achievements, he has an approved patent in the field of Blockchain technology in the event management sector in the India patent office (IPO), and co-authored 3 chapters titled “Gun Tracking System Using Blockchain Technology”, “Secure Event Ticket Booking Using Block-chain Technology”, “Distributed Ledger Technology in the Construction Industry Using Corda” in Blockchain Technology. These chapters are part of “Blockchain Technology: Applications and Challenges”, “Intelligent Systems Reference Library, Springer (WoS and Scopus Indexed)”, and “The New Advanced Society: Artificial Intelligence and Industrial Internet of Things Paradigm, Willey Press (U.S.A)”. He is currently working on other research papers on the Distributed Ledger Technology.

Mr. Vihas Naman is a researcher in the Department of Computer Science and Engineering at ICFAI Foundation for Higher Education, IcfaiTech (Faculty of Science and Technology), Hyderabad, India. His current area of interest for research includes blockchain technology, Ethereum, Distributed Ledger technology, Corda, and the Internet of things. As a part of his achievements, he has an approved patent in the field of Blockchain technology in the event management sector in the India patent office (IPO), and co-authored 3 chapters titled "Gun Tracking System Using Blockchain Technology", "Secure Event Ticket Booking Using Block-chain Technology", "Distributed Ledger Technology in the Construction Industry Using Corda" in Blockchain Technology. These chapters are part of "Blockchain Technology: Applications and Challenges", "Intelligent Systems Reference Library, Springer (WoS and Scopus Indexed)", and "The New Advanced Society: Artificial Intelligence and Industrial Internet of Things Paradigm, Willey Press (U.S.A)". He is currently working on other research papers on the Distributed Ledger Technology.

Ms. T. Kundana is a researcher in the Department of Computer Science and Engineering at ICFAI Foundation for Higher Education, IcfaiTech (Faculty of Science and Technology), Hyderabad, India. Her research interest includes Network Security, Cloud Computing, Machine Learning and Cyber Security.

Mr. D. Abhinav is a researcher in the Department of Computer Science and Engineering at ICFAI Foundation for Higher Education, IcfaiTech (Faculty of Science and Technology), Hyderabad, India. His research interest includes Network Security, Cloud Computing, Machine Learning and Cyber Security.

Ms. P. Sushrutha is a researcher in the Department of Computer Science and Engineering at ICFAI Foundation for Higher Education, IcfaiTech (Faculty of Science and Technology), Hyderabad, India. Her research interest includes Network Security, Cloud Computing, Machine Learning and Cyber Security.

Ms. Sai Lalitha Sunaina M is a researcher in the Department of Computer Science and Engineering at ICFAI Foundation for Higher Education, IcfaiTech (Faculty of Science and Technology), Hyderabad, India. Her research interest includes Cloud Computing, Machine Learning and Data Analytics.

Ms. Neha Pavuluri is a researcher in the Department of Computer Science and Engineering at ICFAI Foundation for Higher Education, IcfaiTech (Faculty of Science and Technology), Hyderabad, India. Her research interest includes Cloud Computing, Machine Learning and Data Analytics.

Mr. Govind Ch is a researcher in the Department of Computer Science and Engineering at ICFAI Foundation for Higher Education, IcfaiTech (Faculty of Science and Technology), Hyderabad, India. His research interest includes Cloud Computing, Machine Learning and Data Analytics.

Mr. Raghavender Rao Jakileti is a researcher in the Department of Computer Science and Engineering at ICFAI Foundation for Higher Education, IcfaiTech (Faculty of Science and Technology), Hyderabad, India. His research interest includes Cloud Computing, Machine Learning and Data Analytics.

Ms. Indrani Inapakolla is a researcher in the Department of Computer Science and Engineering at ICFAI Foundation for Higher Education, IcfaiTech (Faculty of Science and Technology), Hyderabad, India. Her research interest includes Cloud Computing, Data Analytics and Data Visualization.

Mr. SVB Revanth is a researcher in the Department of Computer Science and Engineering at ICFAI Foundation for Higher Education, IcfaiTech (Faculty of Science and Technology), Hyderabad, India. His research interest includes Cloud Computing, Data Analytics and Data Visualization.

Mr. Siliveru Akhil Durga is a researcher in the Department of Computer Science and Engineering at ICFAI Foundation for Higher Education, IcfaiTech (Faculty of Science and Technology), Hyderabad, India. His research interest includes Cloud Computing, Data Analytics and Data Visualization.

Mr. A. D. Sriram Kumar is a researcher in the Department of Computer Science and Engineering at ICFAI Foundation for Higher Education, IcfaiTech (Faculty of Science and Technology), Hyderabad, India. His research interest includes Cloud Computing, Machine Learning, Industry 4.0 and IoT.

Ms. D. MAHESHWARI is a researcher in the Department of Computer Science and Engineering at ICFAI Foundation for Higher Education, IcfaiTech (Faculty of Science and Technology), Hyderabad, India. Her research interest includes Cloud Computing, Machine Learning, Industry 4.0 and IoT.

Ms. B. Rahini is a researcher in the Department of Computer Science and Engineering at ICFAI Foundation for Higher Education, IcfaiTech (Faculty of Science and Technology), Hyderabad, India. Her research interest includes Cloud Computing, Machine Learning, Industry 4.0 and IoT.

Ms. Ramya Reddy P is a researcher in the Department of Computer Science and Engineering at ICFAI Foundation for Higher Education, IcfaiTech (Faculty of Science and Technology), Hyderabad, India. Her research interest includes Cloud Computing, Machine Learning and Artificial Intelligence.

Ms. Lavanya Reddy P is a researcher in the Department of Computer Science and Engineering at ICFAI Foundation for Higher Education, IcfaiTech (Faculty of Science and Technology), Hyderabad, India. Her research interest includes Cloud Computing, Machine Learning and Artificial Intelligence.

Ms. M. Vaishnavi is a researcher in the Department of Computer Science and Engineering at ICFAI Foundation for Higher Education, IcfaiTech (Faculty of Science and Technology), Hyderabad, India. Her research interest includes Cloud Computing, Machine Learning, Vanet and Network Security

Ms. K. Sahaja is a researcher in the Department of Computer Science and Engineering at ICFAI Foundation for Higher Education, IcfaiTech (Faculty of Science and Technology), Hyderabad, India. Her research interest includes Cloud Computing, Machine Learning, Vanet and Network Security

Sachi Nandan Mohanty, Sirisha Potluri, V. Bhanu Prakash, B. Srinath, B. Manjunath

Cloud Security Concepts, Threats and Solutions: Artificial Intelligence Based Approach

Abstract: Artificial intelligence is an advanced technology that helps companies to manage complex operations efficiently and improve productivity. In this generation, many business communities are using AI-based networks to maximize organizational performance but also to evade risks and threats. Security and privacy are both major issues with AI technology that contributes to data privacy and leads to hacking problems. The proposed study focused on security issues of AI technology and explored effective counter measures to improve data privacy. Privacy-preserving cooperative filtering recommendation systems are aiming to supply users with correct recommendations to maintain bound assurances regarding the privacy of their information. This survey examines the latest literature on collaboratively secured collections, provides an overview of the sector and distinguishes significant contributions. The study also focuses and comforts to identify the kind of vulnerability they address and also the form of approach they use to handle it.

Keywords: Cloud Computing, Cloud Security, User Identification System, Data Storage, Data Integrity, Artificial Intelligence

Sachi Nandan Mohanty, Department of Computer Engineering, College of Engineering Pune, Wellesley Rd, Shivajinagar, Pune, Maharashtra 411005, India, sachinandan09@gmail.com
Sirisha Potluri, Department of CSE, IcfaiTech (Faculty of Science and Technology), ICFAI Foundation for Higher Education, Donthanapally, Shankarpalli Road, Hyderabad, Telangana 501203, India, sirisha.vegunta@gmail.com
V. Bhanu Prakash Reddy, Department of CSE, IcfaiTech (Faculty of Science and Technology), ICFAI Foundation for Higher Education, Donthanapally, Shankarpalli Road, Hyderabad, Telangana 501203, India, bhanu.vangati@gmail.com
B. Srinath, Department of CSE, IcfaiTech (Faculty of Science and Technology), ICFAI Foundation for Higher Education, Donthanapally, Shankarpalli Road, Hyderabad, Telangana 501203, India, srinathbellamkonda14@gmail.com
B. Manjunath Reddy, Department of CSE, IcfaiTech (Faculty of Science and Technology), ICFAI Foundation for Higher Education, Donthanapally, Shankarpalli Road, Hyderabad, Telangana 501203, India, manju.chikku55@gmail.com

https://doi.org/10.1515/9783110732573-001

1 Introduction

Cloud Computing is one of the pioneers to add to the field of computer technology in recent times to redesign the possession value using pay-as-you-go model. However, in terms of security, the current methods: anti-virus programs, authentication mechanisms, firewall safety features do not appear to be able to withstand the severities of threats.

Therefore, the user identification system, registers user activity to investigate system performance, adds a protection system in an efficient and collaborative way which is combined with latest practices to provide increased security. Our work focuses on developing an efficient user identification program to exploit the environment in normal way and course of conduct (of the user identification program) and proposes an efficient replacement hybrid approach, which will bring a comprehensive user safety identification program in cloud computing [1-3].

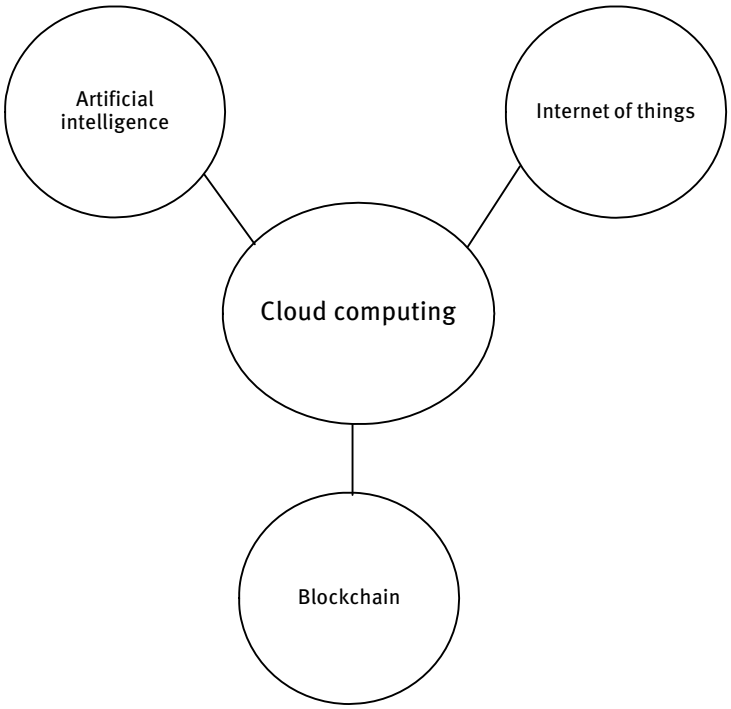

Fig. 1: Emerging research areas of cloud computing

The utilization of proposal frameworks has improved significantly in recent times. Shopping malls present their clients recommendations with suggestions based on

set of past experiences and socio-economic status; Film and book recommendation sites are consistently used to select new top choices of their viewers and readers; online music streaming management generates dynamic playlists to suit the trends of their listeners.

It is magnificent that the new era of history and new technological change is on the rise in every platform. We tend to believe that a new era of "Internet and artificial intelligence (AI)", characterized by ubiquitous networks, data technologies, shared services, border integration, automation, and mass production is coming. The rapid development and integration of the latest AI and web technologies, new data technologies, new energy technologies, mechanical technologies, and biotechnology are a necessary requirement in this new era, which can transform models, methods and natural resources, welfare and national security.

Cloud platform provides significant services such as software package resources with many benefits such as data storage, server maintenance and accessibility for cloud tip users using data access. Due to the rising popularity of the cloud, a large number of databases have been exported to reduce the amount of storage and cost. In addition, data integrity (DI) is an ongoing problem in the cloud to deal with data security and data consistency. Therefore, data usage (DU) face the risk of using cloud computing for storage and data transfer applications, due to the shortage of DI. For the purpose of partitioning the DI problem, the cloud has a high reliability band using trusted third party based encryption scheme (TTP). The TTP function is to ensure continuous DU authentication with continuous DI protection. To ensure data privacy, cloud must use efficient data encryption methods.

Cloud Computing is an expanding field in the area of computing. It is a way to increase resource usage and computing power without having the financial burden of buying new infrastructure on the users. Cloud computing services witnesses many features such as efficiency, reliability, flexibility, profitability, elasticity, availability and on demand assets delivery using utility computing. Cloud resources are usually measured based on their usage to complete the execution of the tasks in the given assignment.

Cloud computing provides services through internet and web applications. Resources dynamically go up or down based on the demand and in addition to that cost efficient pricing is followed by a simple payment policy by using pay as you go model. Therefore, cloud computing platform has several resources which are provided by cloud service provider and the cloud storage processes are changing dynamically to meet the demands of ongoing data and information growth. However, the benefits of cloud storage go progressively with a group of cyber security related protocols and methods.

The privacy issue is one of the most serious threats to data loss, malicious alterations, server crashes with other cyber threats samples such as Yahoo's 3 billion account exposure by hackers in 2013, Apple's iCloud leak in 2014, infringement of information privacy of Drop box In 2016, a leaked iCloud event, wherever the vari-

ous photos of Hollywood actors were unveiled and caused a lot of outcry. Those events have a profound effect on the company's reputation.

Fog integration includes the cloud computing paradigm to the edge of the network, thus providing a new type of applications, services and security in the cloud environment. Therefore, we are often ready to develop cloud technology with protected and secured user information using artificial intelligence mechanisms.

2 Literature Analysis

Artificial intelligence is one of the siginificant research area related to cloud computing. Emerging research areas of cloud computing are artificial intelligence, blockchain and internet of things as shown in fig. 1. The importance and significance of our research is to determine safety risks and problems associated with AI technology and explore the results of recent studies.

2.1 Significance of artificial intelligence

Čerka, Grigienė, and Sirbikytė, (2015) examined that security is a necessary part of AI technology to detect and handle whenever hackers transmit unwanted signals and reduces the data privacy and security related issues. Within organizations, AI technology helps to perform tasks effectively but the presence of unauthorized signals will violate data privacy and lead to data breach problems.

Three key expertise that lead to privacy preservation using artificial intelligence are deep learning, natural language processing, machine learning, neural networks and computer vision. Improper configuration of unauthorized activities and services owned by various cloud devices and infrastructure are efficiently addressed by AI based mechanisms. It is important to use secure networks to handle malware transmission in cloud computing environement where the privacy of AI networks can be increased and the performance of advanced systems can be enhanced.

Guihot, Matthew, and Suzor, (2017) provided their views and stated that AI technology helps to improve business process, and to handle data related risks, challenges and breaches in organizations. Network based AI uses the internet connection and communication systems where some times the presence of unauthorized signals can lead to cybercrime and results into reducing the privacy of sensitive information. If the malware is transmitted and enters into AI based cloud systems, identification, control and handling such transimission is handled by using AI based mechanisms [4-7].

2.2 Security issues

Pan, (2016) determined that there are variety of security risks or issues that occur within the AI networks like security threat of technology abuse, induced by technical defects and plenty of similar issues. It's necessary to seek out the danger factors coupled with cloud computing environment so as to defend these cyber-crimes and risks from the developed systems using AI technology [8].

2.3 Privacy issues

According to Rehman, and Saba, (2014) the privacy of artificial intelligence is often broken by interference communication channels and accessing personal networks of the organizations. Within the advent of artificial intelligence, various privacy risks such as confidentiality problems, phishing, and unauthorized signals transferred by the criminals are handled more efficiently when compared with the existing solutions. Therefore, it is significant to specialize in privacy whereas implementing AI networks in the organizations should guarantee data security and prefer to use solely private networks instead of third parties [9].

2.4 Security and privacy enhancement using artificial intelligence

Artificial Intelligence (AI) goal is to create IoT based infrastructure and fog nodes that monitor the work environment and continuously adapt to provide superior QoS features, reduce the consumption of power and total infrastructure cost.

AI constitutes of various search algorithms, machine learning, and reinforcement learning to efficiently handle issues and problems in cloud. In today's world of deep data operations with fog growth and cloud deployment, more and more AI is needed at different levels to provide better workflow decisions, VM migration, etc. to improve the previously mentioned conditions.

There are many projects aimed at investing in AI strategies to increase the performance of cloud and fog systems. Completely different functions apply directly to cloud planning policies, virtualization algorithms, distribution systems etc. which uses the search methods such as genetic algorithms, supervised machine learning and robust in-depth learning to perform their intended functions.

AI delivers an effective way to optimize large systems with more detail in simplicity of engineering and efficiency by permitting automated decision-making rather than man-made solutions that provide more efficient and faster resolutions.

With the current expansion of the internet, the existence of sensors in the universe, the emergence of big data, the development of e-commerce, the growth of the

information society, and the integration of data and information with the society, the physical environment, and cyberspace, the information environment: AI 2.0 (Pan, 2016) observes great changes in cloud. The arrival of latest technologies empowers a new phase of AI. Key features of AI 2.0 include the emergence of visual acuity driven by in-depth learning data, internet-based intelligence, human and technology-based mechanisms, and high-level media thinking (Pan, 2016).

The continued emergence of smart cities, robots in medical care, automated transport, virtual assistants, mechanical device, automated cars, smart phones, smart toys, smart communities and smart economies provide a wider market demand which urges for the new developments in both AI technologies and applications.

The functions of learning, understanding, making decisions, solving problems and spontaneous thinking such as human thinking is called Artificial Intelligence. The various methods of AI are: fuzzy programs (powerful for language representation), artificial neural networks (which mimic the structure of the human brain; contain highly complex connections of simple mathematical units representing complex problem-solving tasks), genetic algorithms (on purpose of the evolution of human genes to find the right solution) etc. provides machine learning and automation solutions for problem solving [10].

Cloud computing is growing rapidly, and CDC (Centralized Data Center) have become an integral part of prominent industries such as Amazon, Apple, Microsoft, Google, IBM, Facebook. However, it is burdensome to monitor the operations of large data centers manually.

Yotascale is a next-generation computing and automated performance monitoring solution to reduce human response. Yotascale uses historical data to make predictions or decisions about cloud costs using artificial intelligence and helps to save lot of expenditure. In addition, real-time analysis can be done using Yotascale to detect unfavorable trends using in-depth reading strategies (supervised/unsupervised or forecasting models) and find the cause and provide future predictions based on cloud usage and its cost. Research specialization in distributed and cloud computing are given shown in fig. 2 and fig. 3.

In Artificial Intelligence, ANN- artificial neural network is one of the best classification method can be used as an intrusion detection system. Artificial neural network is an efficient information processing method that is motivated by the natural and biological nervous structure. It tries to signify the physical brain, functionality and its thinking process by means of a network, electronic circuit and set of programs.

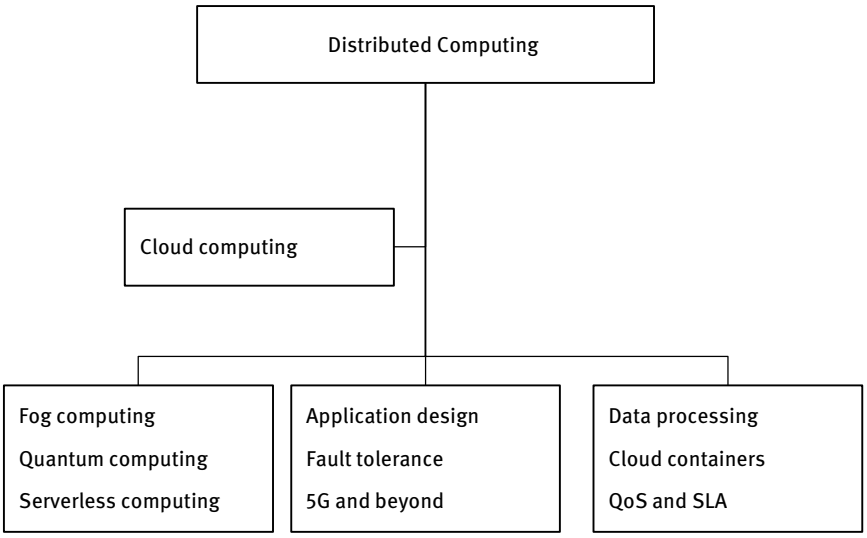

Fig. 2: Research specialization of distributed computing

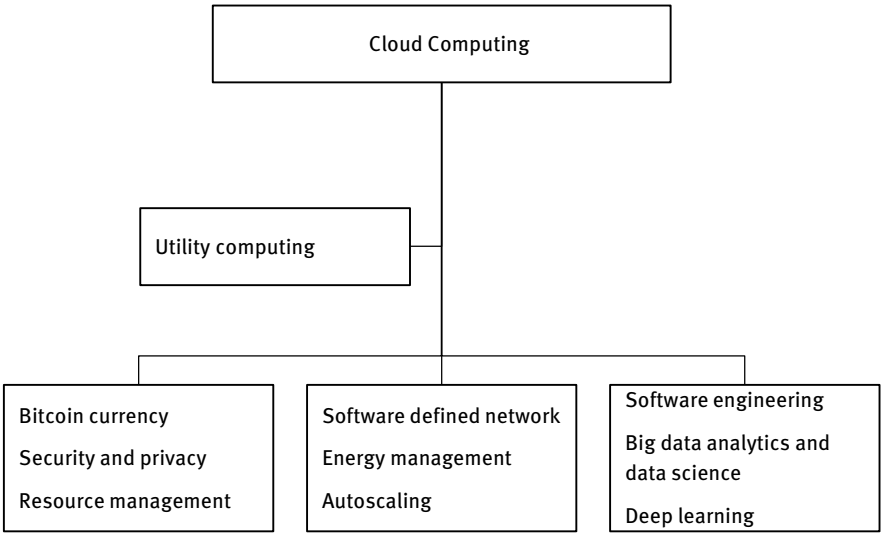

Fig. 3: Research specialization of cloud and utility computing

AI technology facilitates the development of new models, methods, and forms, system design, and technology systems in the field of intelligent production. AI is used in the intelligent manufacturing sector with an intelligent production system. The use of AI beyond the intelligent production system makes no sense. Against the

background of 'Internet plus AI', an intelligent production system characterized by independent intelligence, communication, collaboration, learning, analysis, understanding, decision-making, control and humanization, machine, material, environment and knowledge throughout the system and life cycle.

3 Security

Security is a major factor to consider while adapting to the cloud. Users will store a lot of secure information on their computers. When using cloud computing technology this data will be transferred from their computer to the cloud. Therefore, the cloud must have effective security measures to protect this data. Threats and attacks observed in cloud computing are shown in fig. 4.

Pan, (2016) determined that there are a number of security risks or problems that occur in the AI networks such as security threat of technology abuse, induced by technical defects and many more. It is important to find the risk factors linked with AI technology in order to defend cyber-crimes and risks from the developed systems. From recent literature, it is found that AI is a neutral technique that connects numbers of technologies and computing devices to each other for performing operations effectively [11].

The following are list of security issues observed in cloud computing and same can be efficiently addressed by artificial intelligence practices.

- Control management
- Risk management
- Compliance
- Vulnerability management
- Patch management
- Physical security
- Data security
- Operational security
- Legal issues
- Identity management
- Application security
- Storage security
- Network security
- Information security
- Cyber security
- Virtualization security
- Auditing and maintenance
- Data encryption and key generation

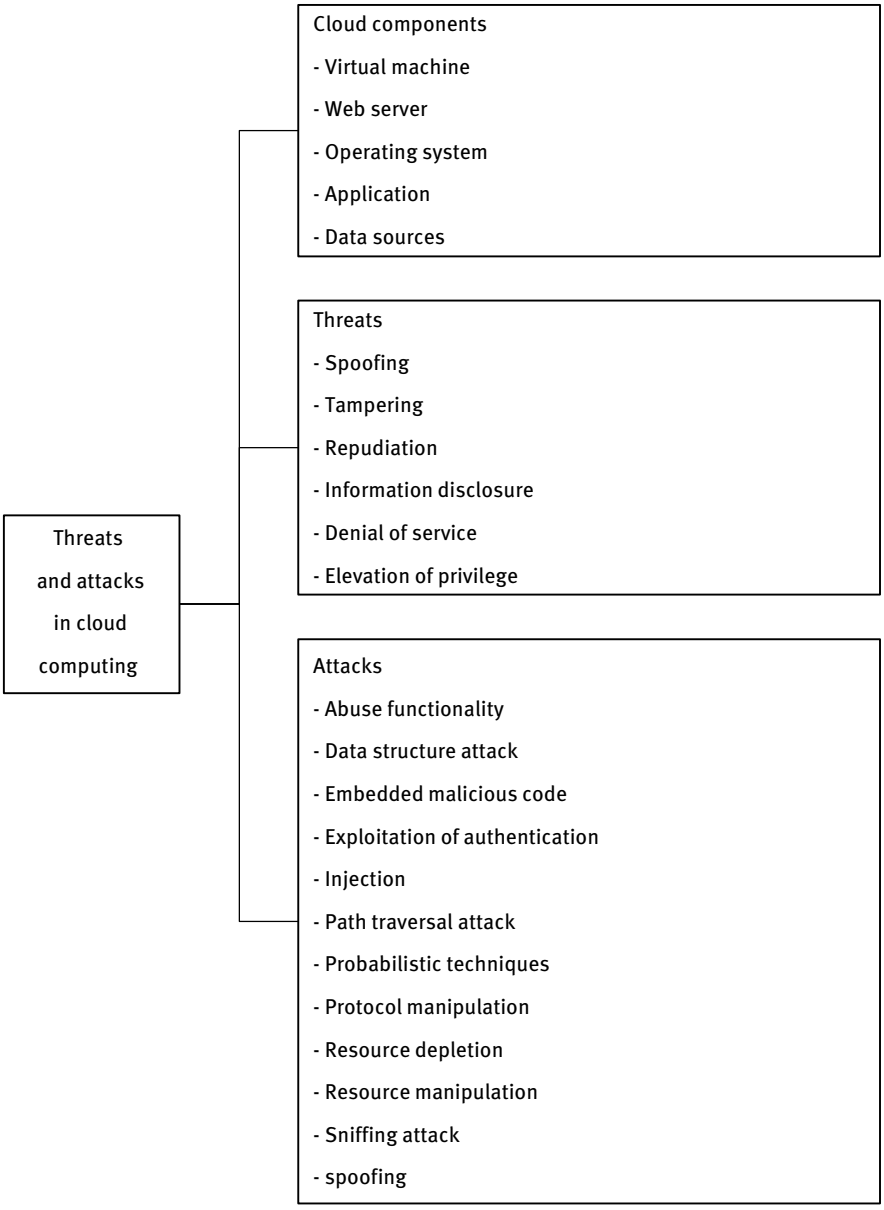

Fig. 4: Threats and attacks observed in cloud computing

Most of the companies suffer cyber-attacks due to technology abuse where the criminals transfer unwanted signals and impact on the developed systems by which the sensitive data can be leaked. Pesapane, et al., (2018) identified that criminals use

malicious programs for transferring fraud signals that help to reduce the performance of the communication channels and technologies used in the AI systems are not able to detect unwanted signals by which hackers can perform data breach. Because of some technical defects, the AI networks are not capable to protect data against cyber-crimes and more than 34% of the companies are facing such problems.

Ransbotham, et al., (2017) supported the argument and examined that lack of awareness is a key problem where companies do not provide complete training to the employees wherein hackers can obtain login credentials of computing devices using malicious programs.

Cloud computing has advantages such as easy implementation, accessibility, distribution, reliability, error tolerance, shared resources, increased storage capacity and cost-saving technology. While Cloud computing has many advantages, it still suffers with many security issues and violations with respect to both cloud service providers and cloud users.

According to a Cloud Security Alliance article, "Data breaches, unfortunate information, recording or administrative tasks, unauthorized integration with Application Programming Interfaces (APIs), DoS attacks, bad content, cloud abuse, inefficiency due to inefficiency, eventually shared new risks", are identified as the top nine threats to cloud computing. Significance of AI in cyber security is shown in fig. 5.

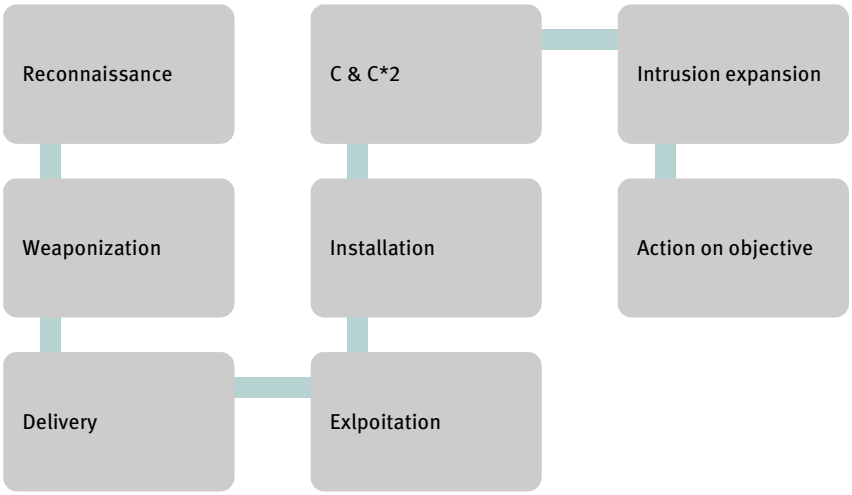

Fig. 5: Significance of AI in cyber security

4 Privacy

Privacy and security often confuse words. Data security ensures that data is available when those with authorized access need it. Data privacy ensures that data is used properly. Privacy is defined as the individual's right to determine how and to whom information is transmitted. Data privacy can be protected by restricting access to data through access control methods or by anonymously disclosing information.

A lot of research on the topic of privacy protection has been done and in recent years, there are a number of important review topics that analyse data confidentiality, privacy protections, proposed structures, and data privacy measures; their pros and cons are published. Suggested methods of data privacy protection are divided into initial methods, statistical analysis used, helpful computer-based information, and machine learning methods.

The privacy of artificial intelligence can be violated by blocking communication channels and accessing corporate private networks. In the area of artificial intelligence, there are three major privacy risks that have taken place including privacy issues, identity theft crimes, and unauthorized signs transmitted by criminals. Therefore, it is important to focus on privacy while using AI networks in business and companies should ensure that they only use independent networks rather than third parties [12].

In order to effectively solve the data privacy protection problem, encrypted storage of cloud data is a very outstanding solution. After encryption, the data is stored in the server provided by cloud service provider in the form of ciphertext, and in the meantime, the server is also required to return the data to user when the user requires. When the user needs to use the data frequently, it requires a lot of network bandwidth and user's time to conduct communication with the server and realize data encryption and decryption, which will significantly reduce the usability of cloud computing.

In the meantime, after the encrypted data stored in cloud server has developed to a certain scale, effective retrieval of encrypted data has become a new problem that needs to be solved, while the traditional information retrieval technology can no long satisfy the requirement of mass data retrieval in the cloud storage environment.

The homomorphic encryption technology is an encryption method which can directly process the encrypted data, and it can effectively protect the security of user's data content, which has very broad development potential under the background of cloud storage application.

By utilizing the homomorphic encryption algorithm, it can not only ensure that the encrypted data won't be statistically analysed to decrypt corresponding plaintext, but also conduct homomorphic operation (such as addition and multiplication) to the ciphertext, while maintaining corresponding plaintext order of this ciphertext during operation.

During the retrieval process, the used index file and keyword are both in the form of ciphertext, and the cloud server cannot obtain any information of user data from the retrieval results. The index file is small, which will not increase the storage pressure of cloud server. In the meantime, the retrieval speed is fast, and it supports retrieval of multiple keywords, which will be convenient for the users and provides high security and strong practicability. Significance of AI in cyber safety in fig. 6.

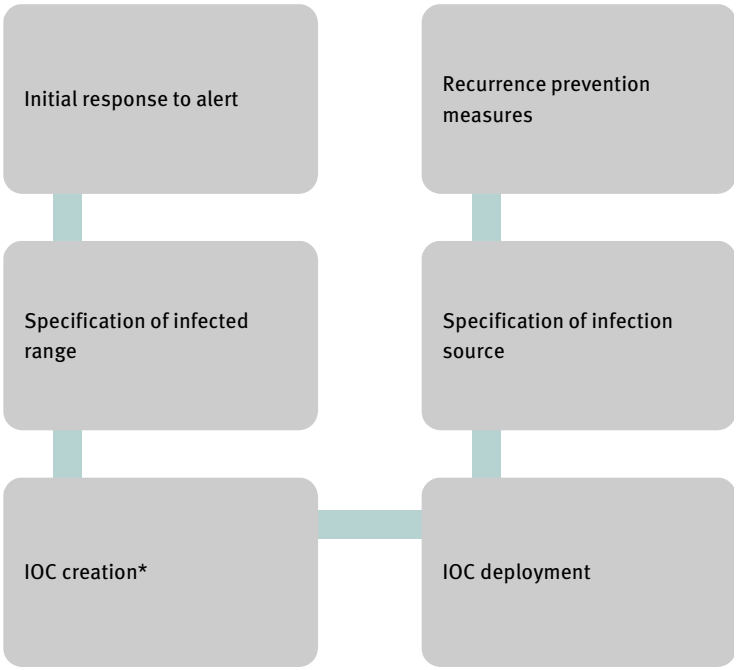

Fig. 6: Significance of AI in cyber safety

The following are list of privacy issues observed in cloud computing and same can be efficiently addressed by artificial intelligence practices.

- Loss of control
- Information misuse
- Physical risk
- Identify theft
- Privacy related to internet based activates
- Privacy laws
- Network suspicious activity
- Information hacking
- Data privacy

5 Security and Privacy Solutions Using Artificial Intelligence

Artificial Intelligence is an advanced technology that helps companies manage complex operations efficiently and improve productivity. In this generation, many business communities are using AI-based networks to maximize organizational performance but also face risks and threats. Security and privacy are both major issues with AI technology that contributes to data privacy and leads to hacking problems. The proposed study focused on security issues of AI technology and explored effective countermeasures to improve data privacy [13-15].

There are following countermeasures and strategies can be used for addressing security threats in artificial intelligence:

- Avoid unwanted and unauthorized signals from the systems
- Only use secure networks and protect advanced systems
- Install effective security tools like firewall and data encryption
- Provide complete training to the employees related to AI based networks
- Develop and implement privacy policies
- Using anti-phishing techniques and tools

6 Proposed Solutions or Approaches

6.1 Research method

It is a large part of research-focused on research quality and questions related to the topic of research. There are two methods used as research methods namely inclination and extraction. Import is used to provide depth details related to the research topic while the pull method is used to give brief details on investigation. In this study, the import method is used because of its ability to deliver practical points related to cloud security. With the help of such method, various research questions can be successfully resolved in order to find reliable facts related to the research topic.

6.2 Research design

It is a useful tool that provides proper research and management of research issues successfully related to the research. Two types of designs used in the study are namely quality and quantity. Russell, Dewey, and Tegmark, (2015) checked that quality is used to collect doctrinal facts however the plural is used to obtain statistical data in the study. In this study, quality construction is acceptable because of

ownership of the research topic and the ability to provide depth details related to artificial intelligence protection. It uses in such a way that the quality of research is also improved to get the right points.

6.3 Data collection

There are two parts of data collection methods including basic and secondary. Scherer, (2015) pointed out that the primary method provides new information but the second method provides reviewed data and facts in the study. In this study, the second method was adopted to collect information about artificial intelligence. To find the second data book updates various sources such as data collected in recent, online papers websites, and books are used.

6.4 Data analysis

In this investigation, a descriptive content method is used to analyse the data being collected because it can provide effective results and points related to the research topic. In addition, Excel software is used to represent data collected into tables and graphic forms. Therefore, the use of such methods has been improved research questions resolved and managed the flow of details.

Artificial intelligence technology can be used to take action and it has already been used to detect malware, and its functionality has already been established. Another proof of its effectiveness is that in July 2017 Google announced that they will integrate Cylance AI technology into VirusTotal - a Google malware detection service. IBM is also trying to demonstrate the effectiveness of its AI technology with intelligent search engines that carefully control the vast amount of threatening information using Watson's cyber security.

For privacy-preserving analysis of big data confidentiality, an in-depth learning approach is proposed. The method converts the critical part of personal information and it has become sensitive information. To perform this process, a two-stage method is proposed namely modified sparse autoencoder types and CNN have been used in architecture.

A modified denoising autoencoder enables data conversion and CNN sets the path to modified data. To achieve a lower loss in data conversion, a sparsification parameter was added to it specifically autoencoder function with Kullback split function - Leibler.

Here, efficiency of the model is performed by the MSE (mean square error) function of the loss. To test the accuracy of the transformation process, features based sparse denoising autoencoder algorithm fed on the installation of CNN's advanced

algorithm and reconstructed data classification. Reconstructed data classification is included in the classes specifically black (0), white (1) and gray (2).

CNN algorithm is classified by Black class data as Gray class with details of 0.99. Comparisons of the proposed method with an efficient autoencoder are also provided and used in Cleveland's medical database extracted from the databases of cardiovascular disease, Arrhythmia and Skoda data sets have shown that the proposed method exceeds other standard methods.

7 Model/Data Theft Security Technology

7.1 Private separation of teacher ensembles (PATE)

This technology works by dividing training data into multiple sets in the model training category, each training category is an independent DNN model. Independent types of DNN are used to jointly train student model by voting. This technology ensures that student's mind model does not disclose specific training data, thus ensuring the confidentiality of training data.

7.2 Unique privacy protection

This technology adds audio to data or models using different privacy in the model training phase. For example, some experts suggest how to make gradients by means of alternative privacy measures to protect the privacy of data.

7.3 Model watermarking

This technology integrates special recognition neurons into the original model on the model training phase. These neurons enable a special input sample to test whether another model has been detected by stealing the original model.

8 Why is AI Technology Essential for Cybersecurity?

Cyber-attacks are increasingly varied. While there are still many indiscriminate attacks such as malware transmission and fraudulent emails, sophisticated attacks targeting them make it clear that targeted intentions are now a major threat. Cyber-attacks in recent years have been hampered by their highly organized and industrialized structures. Personal information and various types of malware used for tar-

geted attacks are widely available, readily available, and inexpensive on the black market to facilitate the identification and use of weapons are the first stages of cyber-killing series.

Now, hackers enjoy a situation where they can launch multiple targeted attacks in a short period of time using the tools available on the black market. This has blurred the line between indiscriminate attacks and targeted attacks. It is now understood that normal human resources and response speed will not be able to keep pace with the rapid changes in cyber-attacks. This is a vision that leads security professionals to place their trust in AI technology where rapid progress is being made.

In terms of improving efficiency and faster response, efforts are being in progress to provide a type of solution called security orchestration and automation (SOA) for attracting attention in the United States since about 2014 and the Hexadite of Israel. In SOA, anti-defence strategies called playbooks are described in advance. In line with these processes, SOA can automatically perform data collection, analysis, and implementation of resistance measures as shown in fig. 5 and fig. 6. Here again, AI is expected to play a key role in dynamic planning and revitalization of playbooks.

9 Results

The proposed study provides details about implants intelligence and their security concerns against companies. It turns out that AI is an efficient technology that helps companies to solve complex tasks reliably. Safety is the big deal of anxiety associated with assisted artificial intelligence technology because criminals have to obtain sensitive information and access to computer devices of companies. A review of the literature done and shows that ignorance is a major problem with employees as a result they can use unauthorized networks in computer programs as well as suffers from data breach problems.

It is found that selected search terms have been provided full details regarding the security of artificial intelligence. A big part of artificial intelligence is that it connects a person, mechanical equipment etc. so that companies can work with a number of jobs simultaneously. Therefore, it is important for companies to use appropriate safety tools while operating artificial intelligence at work and employees do not know about security attacks related to computer devices. Available that there are three safe attacks that occur in the implant site.

Fraud includes malware, identity theft, and refusal to work on attack. The proposed study provided effective combat strategies which can be used to address privacy concerns and connected security issues with artificial intelligence technology. Data security and privacy is ensured with efficient data encryption and

decryption algorithms. With AI integration, security and privacy can be heightened to the next level. Code for reverse cipher and Caesar cipher algorithms are given as shown below. Flowchart for data encryption and decryption is given in the fig. 7.

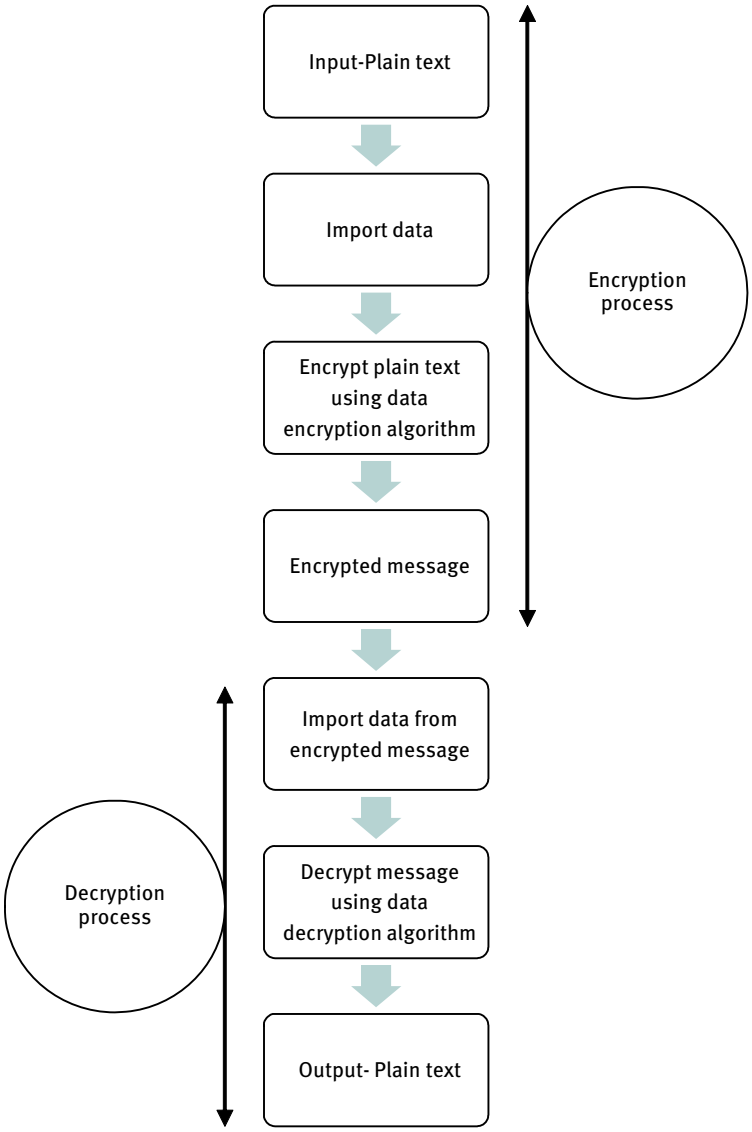

Fig. 7: Data encryption and data decryption process

Listing 1: Code for reverse cipher and Caesar cipher algorithms

```
#Code for reverse cipher algorithm
message_var = "Demo on reverse cipher"
translated_var = " "
it_var = len (message_var) - 1
while it_var >= 0:
    translated_var = translated_var + message_var [it_var]
    it_var = it_var - 1
print ("Cipher text with cipher algo is: ", translated_var)
#Code for Caesar cipher
def encrypt_fun (text_var, s1):
    result_var = ' '
    for it_var1 in range (len (text_var)):
        ch = text_var [it_var1]
        if (ch.isupper ()):
            result_var += chr ((ord (ch) + s1-65) %26+65)
        else:
            result_var += chr ((ord (ch) + s1-97) %26+97)
        return result_var
text_var = "Demo on Caesar cipher"
s1 = 4
print ("Plain text: " + text_var)
print ("Shift pattern text: " + str (s1))
print ("Cipher text: " + encrypt_fun (text_var, s1))
```

10 Conclusion

From the above discussion, it can be concluded that security is a major problem associated with AI technology that helps criminals commit data breaches and hacking activities in companies. This paper provided information about artificial intelligence and examined the security problems associated with AI technology.

It is found that the conducted literature search reviewed each and every point related to the artificial intelligence security attacks. There are numerous attacks occur in AI technology including malware, phishing, and DoS attack that need to be addressed on the priority basis in order to protect private details from the criminals. It is determined that the utilization of firewall and encryption methods can help the companies to protect data against cybercrimes and attacks. The company should provide training to the employees by which they can avoid the involvement of third-party networks and unauthorized signals from the AI-based systems.

With the increasing amounts of data generated by programs, traditional internal access detection systems have worked slower. As a result, applications for artificial intelligence are widespread although they are currently designed for population growth. This is because people believe that they are currently doing more comprehensive tasks than AI goals for detecting, identifying and responding to new cyber threats. There is the concern, however, is that AI tools themselves may be unsafe and attackers may produce AI-powered weapons soon. This is an area of research that needs to continue attention.

The impact of AI on human aspects of information and cyber security is therefore summarized in the present and future conditions. For now, state, the impact of AI on human capital. In the future, however, the impact can go either way; that is, people can be completely replaced by independent AI applications or individuals and AI may be integrated to fill each other with good results. Investigators went into future when the social and technological process is recommended as a solution and needs to continue research in this regard. There is recognition of certain research limitations in all aspects of AI. On the other hand, there are various AI magazines that have not been tested.

This proposed research provided a way where readers can enhance skills in the area of artificial intelligence and resolve the security concerns in an appropriate manner.

11 References

[1] Mazur S, Blasch E, Chen Y, Skormin V, Mitigating cloud computing security risks using a self-monitoring defensive scheme, Proceedings of the 2011 IEEE National Aerospace and Electronics Conference (NAECON), Dayton, OH, 2011, pp. 39-45, doi: 10.1109/NAECON.2011.6183074

[2] Alabdulkarim A, Al-Rodhaan M, Tian Y, Al-Dhelaan A, A privacy-preserving algorithm for clinical decision-support systems using random forest, Computers, Materials & Continua, 2019, Vol.58, No.3, pp.585-601, doi:10.32604/cmc.2019.05637

[3] Chen J, Wang Y, Wang X, On-demand security architecture for cloud computing, Computer, 2012, vol. 45, no. 7, pp. 73-78, doi: 10.1109/MC.2012.120

[4] Li B, Hou B, Yu W et al., Applications of artificial intelligence in intelligent manufacturing: a review, Frontiers Inf Technol Electronic Eng, 2017, 18, 86–96

[5] Rasim A, Ramiz A, Fargana A, Privacy-preserving deep learning algorithm for big personal data analysis, Journal of Industrial Information Integration, 2019, Volume 15, Pages 1-14, ISSN 2452-414X, https://doi.org/10.1016/j.jii.2019.07.002

[6] Sukhpal G, Shreshth T, Minxian X, Inderpreet S, Karan V, Lindsay D, Shikhar T, Smirnova D, Manmeet S, Jain U, Pervaiz H, Sehgal B , Sukhwinder K, Sanjay M, Sadegh A, Harshit M, Stankovski V, Garraghan P, Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges, Internet of Things, 2019, Volume 8, 100118, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2019.100118

[7] Wan J,Yang J, Zhongren W, Qingsong H, Artificial intelligence for cloud-assisted smart factory, IEEE Access, 2018, PP. 1-1, 10.1109/ACCESS.2018.2871724

[8] Chen J, Dongyong Y, Data security strategy based on artificial immune algorithm for cloud computing, Applied Mathematics & Information Sciences, 2013, 7, 149-153, 10.12785/amis/071L21

[9] Sun L, Jiang X, Ren H, Guo Y, Edge-cloud computing and artificial intelligence in internet of medical things: architecture, technology and application, IEEE Access, 2020, vol. 8, pp. 101079-101092, doi: 10.1109/ACCESS.2020.2997831

[10] Tabrizchi H, Rafsanjani K, A survey on security challenges in cloud computing: issues, threats, and solutions, J Supercomput, 2020, 76, 9493–9532, https://doi.org/10.1007/s11227-020-03213-1

[11] Barona R, Anita E, A survey on data breach challenges in cloud computing security: issues and threats, 2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT), Kollam, 2017, pp. 1-8, doi: 10.1109/ICCPCT.2017.8074287

[12] Alia A, Al-Rodhaan M, Al-Dhelaan Y, A privacy-preserving algorithm for clinical decision-support systems using random forest, Computers, Materials & Continua, 2019, 58, 585-601, 10.32604/cmc.2019.05637

[13] Wang T, Jiyuan Z, Chen X, Guojun W, Anfeng L, Yang L, A three-layer privacy preserving cloud storage scheme based on computational intelligence in fog computing, IEEE Transactions on Emerging Topics in Computational Intelligence, 2018, 2, 3-12, 10.1109/TETCI.2017.2764109

[14] Ram P, Murali S, Siva A, Privacy preservation techniques in big data analytics: a survey, J Big Data, 2018, 5, 33, https://doi.org/10.1186/s40537-018-0141-8

[15] Muhammad N, Cloud computing: security issues and challenges, Journal of Wireless Communications, 2016, 1 (1), 10-15, https://doi.org/10.21174/jowc.v1i1.73

Shagun S Lokre, Shanmukhi Priya, Vihas Naman, Sachi Nandan Mohanty, Sirisha Potluri

Addressing Security and Privacy in Cloud Computing: Blockchain as a Service

Abstract: In recent times, the IT industry has been marked as a new era of software advancement with the introduction of cloud computing technology. This technology has become very essential for delivering infrastructure and has been adopted widely due to its performance and availability. Cloud computing allows us to access many applications and services over the Internet. A majority of the activities performed by this technology revolves around different forms of data, making it an invaluable resource. The importance and usage of data have reached new heights and like all precious resources, even data requires security and privacy. Unfortunately, this is an issue that concerns many cloud computing users as the data proprietors cannot have complete control over certain aspects like the location of the data storage and access permissions. Blockchain Technology, one of the emerging technologies can be used to complement the issues concerning cloud users. This technology provides features like decentralization, distribution, authenticity, immutability, trust, etc. that can be used to face the threats of data integrity. In this chapter, we will address the issues concerning the security and privacy of the data in the cloud model and how the features of the blockchain technology can enhance the integrity of this model. Although, there are certain limitations like high latency and low throughput, decreasing the practical utility of blockchain technology

Keywords: Security, Privacy, Cloud, Decentralization, Integrity, Blockchain Technology

Shagun S Lokre, Department of CSE, IcfaiTech(Faculty of Science and Technology), ICFAI Foundation for Higher Education, Donthanpally, Shankarpalli Road, Hyderabad, Telangana 501203, India, shagunslokre22@gmail.com
Shanmukhi Priya, Department of CSE, IcfaiTech(Faculty of Science and Technology), ICFAI Foundation for Higher Education, Donthanpally, Shankarpalli Road, Hyderabad, Telangana 501203, India, shanmukhipriya99@gmail.com
Vihas Naman, Department of CSE, IcfaiTech(Faculty of Science and Technology), ICFAI Foundation for Higher Education, Donthanpally, Shankarpalli Road, Hyderabad, Telangana 501203, India, vihas.naman@gmail.com
Sachi Nandan Mohanty, Department of Computer Engineering, College of Engineering Pune, Wellesley Rd, Shivajinagar, Pune, Maharashtra 411005, India, sachinandan09@gmail.com
Sirisha Potluri, Department of CSE, IcfaiTech (Faculty of Science and Technology), ICFAI Foundation for Higher Education, Donthanapally, Shankarpalli Road, Hyderabad, Telangana 501203, India, sirisha.vegunta@gmail.com

https://doi.org/10.1515/9783110732573-002

1 Introduction

Even before cloud computing was developed, it was the IT industry that faced some tough challenges related to storing and accessing data, hosting, and data privacy to name a few. Before the cloud, client/server computing was essentially centralized storage where all the software, data, and control is located on the server-side. This created a major setback for the IT industry since centralized databases rely heavily on network connectivity, which means the slower the internet connection, the longer the access time for the database is needed. Although data redundancy is limited or no, if a collection of data is lost accidentally, it is very difficult to recover it manually. Earlier if a user desired to view some information or execute a program, he/she would have to connect to the server and then obtain access to it and then do his/her work. That's not all, if the IT firm is huge with a large number of employees then it becomes difficult for the company to arrange adequate hardware and software to carry out their tasks. It is not possible to purchase software and applications for every system and every employee. But it did not take much time to find a solution that changed the face of the IT industry, "Cloud Computing" [1-2]. Cloud computing in simple terms means that the services provided of computer resources are controlled and managed by the cloud provider rather than the end-user. These resources include everything from browser-based web applications, third party data storage devices, or third-party servers used to support an industry, research, or personal project's computer infrastructure.

Before the widespread use of cloud computing, businesses and general computer users usually had to purchase and maintain the software and hardware they wanted to use. Based on the increasing availability of cloud-based apps, storage services, and machines, firms and consumers have access now as Internet services to a wealth of on-demand computing resources [3]. If on-the-job software and hardware are shifted to a remote networked and distributed resource, cloud users are no longer required to invest the work, equity, or expertise needed to buy and maintain the data. This unprecedented access to computer resources has resulted in a new group of cloud-based companies and changed IT practices across industries and turned many computer-aided practices into everyday ones. Many organizations started to use the cloud to store records, supply corporate applications, and deploy services and goods digitally. These kinds of cloud-based technologies and adoptions are unique to the field. In the education world, educators and scholars use cloud-based teaching and research applications [4]. As they say, nothing is perfect in this world, cloud computing has few drawbacks which need to be taken into consideration before moving ahead. In cloud computing, confidentiality and privacy are amongst the most questionable. By the use of cloud storage infrastructure, we are completely committed to providing cloud-based application protection and confidentiality of the data. This means that if we encounter any problem, we cannot

claim damages to the server for data errors or any kind of mistakes in the data. Another major disadvantage in cloud computing is its vulnerability in the event of an attack. There are several concerns about cloud computing since cloud computing is online, any aspect of cloud computing can be exposed to a wide range of servers allowing data attacks and server storage activities. In this chapter, we are going to propose how Blockchain Technology can be useful to make the whole system decentralized, tamper-proof, and transparent [5].

2 Literature Survey

As of now, blockchain technology faces core obstacles related to scalability, regulatory limits, identity registration, consumer protection, laws and regulations, and compliance requirements. This chapter is written based on the literature of the previous research, combines blockchain technology and the concept of cloud to create a secure cloud system with selected access permissions [6]. This chapter consists of a detailed study of the combination of cloud systems and blockchain technology. With the current progress of science and technology, the need for secure and fast systems has become the top priority for any information retrieval. The current uses of blockchain include assistance to an IoT system and cloud computing system assisting blockchain technology to make a home environment more efficient, secure, and faster in terms of any processes, this uses Cloud Service Provider [7], Edge Service Provider, and a Lightweight client; each of these modules assists in the storage and usage of data.

Another application using blockchain is secure network computing for lightweight clients, this application is used for mobile devices that do not have enough computing power for heavy usage [8]. This application uses mobile resource management that connects nearby mobile phones using Bluetooth technology, with the combined resources of the phones nearby we use Secure Authentication Management human-centric Scheme (SAMS) to authenticate mobile devices using blockchain, with all the devices giving authentication data falsification can't take place [9]. The major usage of blockchain technology is the medical sector, the medical history of any patient is really important for the diagnosis of specific illnesses [10]. The easier it is to store and securely share this data as confidentiality is of utmost importance, the easier it is to diagnose and cure any illness. Using a decentralized application, we will upload all the medical history to the blockchain, allowing the patient to grant access to any specific doctor to check and add the diagnosis to the existing data. This concept is known as Electronic medical records. We have also used multiple survey papers related to the security and privacy issues present in cloud computing. There are multiple types of cloud services such as Software, Platform, and Infrastructure as a service [11].

Each of these models has complexities and security issues of its own. The main challenges being confidentiality, Integrity, availability of data [12]. The supporting concept for cloud computing is virtualization, the process which allows easy uploading of data onto any cloud service. There are multiple challenges present in technology related to cloud computing using blockchain. From the blockchain perspective, there are scalability issues. From the cloud computing point of view, there are security problems and financial problems since cloud services can be expensive [13].

3 Cloud Computing Concepts

Before moving ahead with the chapter, one might come across a few questions such as what exactly cloud is? Where is the cloud? Are we currently in the cloud? Cloud computing, in the most simplistic words, means the data and programs are stored and accessible through the Internet rather than the hard disc of our computer. In the end, the term "cloud" is just an internet metaphor. Cloud-based computing encourages files to be saved in a remote archive instead of on a private hard disc or local storage device. Although an electronic computer has access to the Internet, the electronic device has access to the data and the software application. Cloud storage is called as such since the knowledge being viewed can be located directly in a cloud or a virtual environment. Companies that have cloud storage allow users to save files and software on remote servers and then access all data over the Internet. This ensures that the user is not forced to be in a certain position to obtain access to it, enabling the user to operate remotely. Cloud computing eliminates all of the hard lifting involved in crunching and manipulating data from the laptop we hold or sit and operate on. It also transfers the entire job to huge cyberspace computing clusters. The Internet is evolving into a cloud, such that our files and jobs can be viewed from every device in the world, from which we bind to the Internet. Cloud storage platforms provide a range of features for consumers, such as Email, memory, data backup, development of and checking software, data processing, audio and video streaming, distribution of on-demand devices [14].

The services provided by cloud computing is categorized into 3 service models as shown in the fig. 1:

- SaaS: Software as a Service.
- PaaS: Platform as a Service.
- IaaS: Infrastructure as a Service

SaaS: NIST describes this service in cloud as being able to access the provider's cloud computing applications. Applications can be accessed from separate client devices by either a thin client interface such as a web browser or a software inter-

face. With the likely exception of minimum user specific configuration requirements, the user does not track or manage the cloud resources including network processors, operating systems, memory and even individual software functionality.

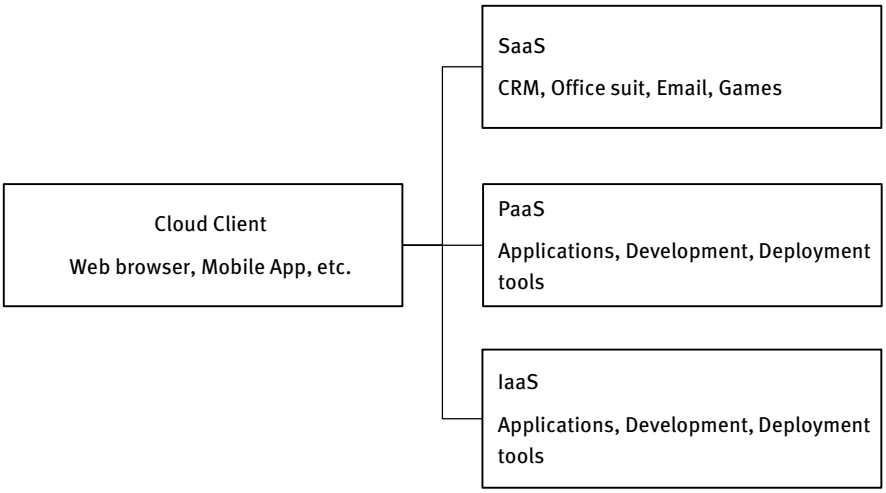

Fig. 1: Categories of cloud computing

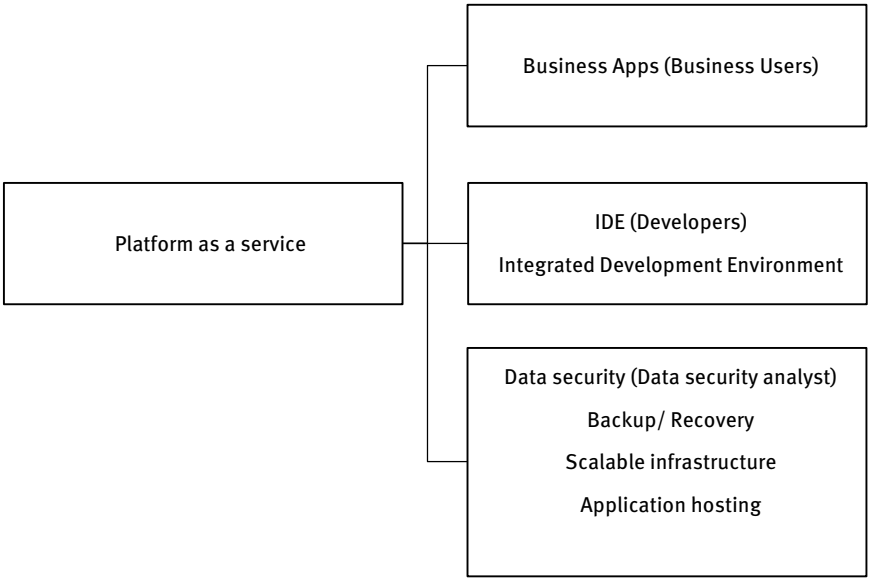

Fig. 2: Platform as a service

Users gain access to application applications and databases as a service (SaaS) model. Infrastructure and systems that run software are operated by cloud providers. SaaS is often referred to as "on-demand software" and is typically priced on a pay-per-use basis or with a monthly fee.

The use of SaaS has proven to be advantageous in terms of scalability, reliability, and performance.

- Modest software tools
- Effective use of software license
- Centralized data and monitoring
- Responsibilities of the network operated by the provider
- Multi-stakeholder solutions

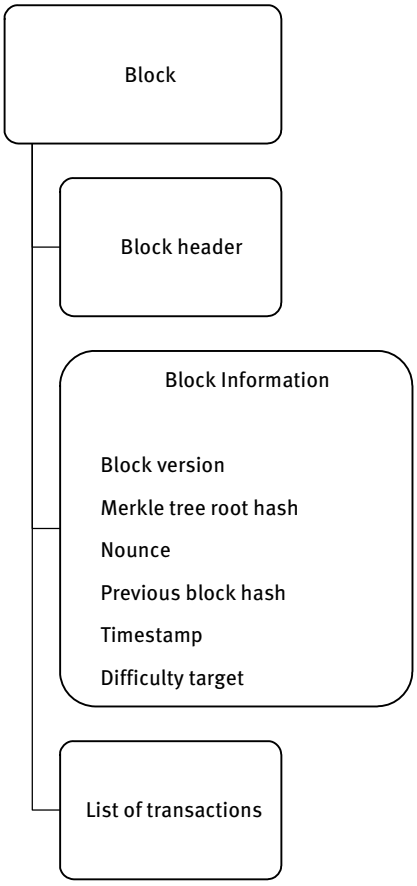

Fig. 3: Block Structure in a blockchain

PaaS: As per NIST, the platform as a service definition in cloud computing is described as: The functionality offered to the user is to execute consumer-created or purchased software to the cloud infrastructure by writing a set of codes, using libraries, APIs, and resources funded by the vendor. The user neither operates nor monitors the underlying cloud resources, including the network, servers, operating systems, or storage, but has control over the software installed and likely configuration settings for the application-hosting environment.

PaaS vendors provide a platform for creating applications as shown in fig. 2. The vendor usually creates a toolkit, implementation specifications and channels for distribution and payment. In PaaS models, cloud vendors include a computing infrastructure, usually providing an operating system, a programming-language execution environment, a database, and a web server.

The benefits of using PaaS include:

- Higher administrative overheads
- Adjustable options
- More modern software for the framework

IaaS: Infrastructure as a Service (IaaS) is an Instant Computing Infrastructure, delivered and operated over the Internet. It is one of four types of cloud computing, along with software as a service (SaaS), application as a service (PaaS), and server less services.

IaaS easily scales up and down with demand, allowing you to pay for what you're using. It lets you escape the cost and difficulty of owning and maintaining your physical servers and other data centre resources. Each resource is provided as a separate service component and you only need to rent a single resource for as long as you need it. The cloud storage vendor, such as Azure, operates the platform when buying, downloading, configuring, and maintaining your software—operating systems, middleware, and programs [15].

4 Consensus Mechanisms

Cloud computing provides multiple advantages when it comes to the business and IT sectors. It allows us to create what is indeed a virtual workplace, so that we can communicate everywhere at all times. With the number of web-enabled gadgets used in today's corporate world (ex. smartphones, tablets), access to your data is now simpler. Moving on to cloud storage will decrease the IT systems administration and maintenance costs. It will reduce the expenses by leveraging the services of the cloud computing platform rather than buy costly systems and appliances for our business. Majority of the companies with more than 1000 employees do not have the same IT requirements as a start-up [16]. Cloud usage is a great choice as it enables

companies to scale up/down their IT divisions efficiently—and quickly—according to market requirements.

Cloud-based applications are suitable for organizations that have rising or evolving demands for bandwidth. You can quickly expand the capability of your cloud without spending on physical resources as your company demands in-crease. This degree of versatility will offer a true edge over competing companies using cloud computing. That's when scalability comes into the picture. Scalability minimizes the risks involved with internal maintenance and organizational challenges. With professional strategies and zero upfront investment, you have high-performance tools at your side. The biggest value of the cloud is undoubtedly scalability [17].

5 Blockchain Technology Concepts

In layman's terms, a blockchain is a chain of blocks that contains data in the form of transactions. Technically, a blockchain is a distributed, decentralized, and trusted ledger or data-sharing platform that can be utilized by participants who do not trust each other. A blockchain is said to be distributed as every participant in the network executes a job collectively and it is said to be decentralized as there are multiple points of coordination, with no single point of failures [18].

In the earlier days, the usage of traditional ledgers resulted in central authority as only one entity would control the entries made into the ledger. But with the introduction of blockchain technology, each participant in the network would have a copy of the ledger and no single participant holds the power to make an entry solely. All the participants follow a consensus mechanism to decide the addition of an entry into the ledger. The most common consensus mechanisms are listed below.

5.1 Consensus mechanisms

A consensus mechanism is an algorithm for fault tolerance that is used by the blockchain technology to accomplish the agreement requirements on an individual data value or a single state of the network amid the participants [19].

– Proof of Work (PoW): This is the most commonly used algorithm these days. This algorithm requires the participants of the network to solve a challenging computational puzzle to create new blocks. The mechanism of solving the puzzle is called "mining" and the nodes that carry out this process are called "miners". The miners who solve this puzzle will get an incentive, known as a block reward. The probability of mining a block depends on the work done by the miner. This work consumes physical resources like CPU power and time.

- Proof of Stake (PoS): This algorithm requires a miner to acquire a sufficient stake to mine a block. While executing an attack is expensive, the incentive for the attack is also reduced as the attacker needs to own a high stake. There-fore, an attack will have more effect on the attacker. This process provides in-creased security and is power efficient but fails to keep the system completely decentralized.
- Proof of Burn (PoB): This algorithm requires the miner to burn some wealth to mine a new block. The miners should show proof that they have burned some wealth by sending coins to a verifiably un-spendable address. This process is expensive like PoW but no external resources are used except the miner's wealth. PoB consumes virtual or digital resources and is power efficient too. PoB works by burning PoW mined cryptocurrencies.

5.2 Structure of blockchain

All blockchain structures are generally categorized into three categories:

- Public blockchain architecture: In this architecture, any participant can enter and exit the blockchain network as per their will, without any permissions. All the willing participants have access to the data in the network as long as they are in the network. Ex: Bitcoin, Ethereum, etc.
- Private blockchain architecture: In this architecture, each participant re-quires permission to enter and exit the blockchain network. The participants who enter the blockchain can be restricted to certain data as well. This system is controlled by the users of a specific organization. Ex: Hyperledger Fabric.
- Consortium blockchain structure: In this architecture, the blockchain net-work is built by a set of organizations. This architecture is neither completely public nor completely private. All the permissions are controlled by the preliminary assigned users. Ex: Quorum, Corda, etc.

The tab.1 gives an outline of the comparison of the three blockchain structures:

Tab. 1: Blockchain structure comparison

Property	Public Blockchain	Private Blockchain	Consortium Blockchain
Accessibility	Anyone	Single organization	Multiple organizations
Who can join?	Anyone	Permissioned and known identities	Permissioned and known identities
Consensus mechanism	Pow/Pos	Voting or multi-party consensus algorithm	Voting or multi-party consensus algorithm

Property	Public Blockchain	Private Blockchain	Consortium Blockchain
Consensus determination	All miners	Within one organization	A selected set of nodes
Consensus process	Permission less	Permissioned	Permissioned
Read permission	Public	Public or restricted	Public or restricted
Immutability level	Almost impossible to tamper	Could be tampered	Could be tampered
Efficient usage of resources	Low	High	High
Centralization	No	Yes	High
Transaction speed	Slow	Lighter and faster	Lighter and faster

Though a blockchain is divided into three categories, all blockchains consist of blocks and all blocks follow a similar structure. A block is like a data structure that accumulates the transactions that would be included in the blockchain [20]. Every block is divided into a block header that contains metadata and a list of transactions as shown in fig. 3. The first block in the blockchain is called the genesis block. A block header consists of:

- Block version: This is a version number that is used to track software updates. Its size is 4 bytes.
- Previous block hash: This is a reference to the hash of the parent/previous block in the current chain. Its size is 32 bytes.
- Merkle tree root hash: This is the hash of the root of the Merkle tree of this block's transactions. Its size is 32 bytes.
- Timestamp: This is the approximate time required to create a block. Its size is 4 bytes.
- Nonce: This is a counter used for the proof-of-work algorithm. Its size is 4 bytes.
- Difficulty target: This is the proof-of-work algorithm difficulty target for this block. Its size is 4 bytes.

The mining process requires the nonce, the difficulty target, and the timestamp.

5.3 Workflow of blockchain

Fig. 4 depicts the workflow of a blockchain that utilizes the proof-of-work consensus mechanism.

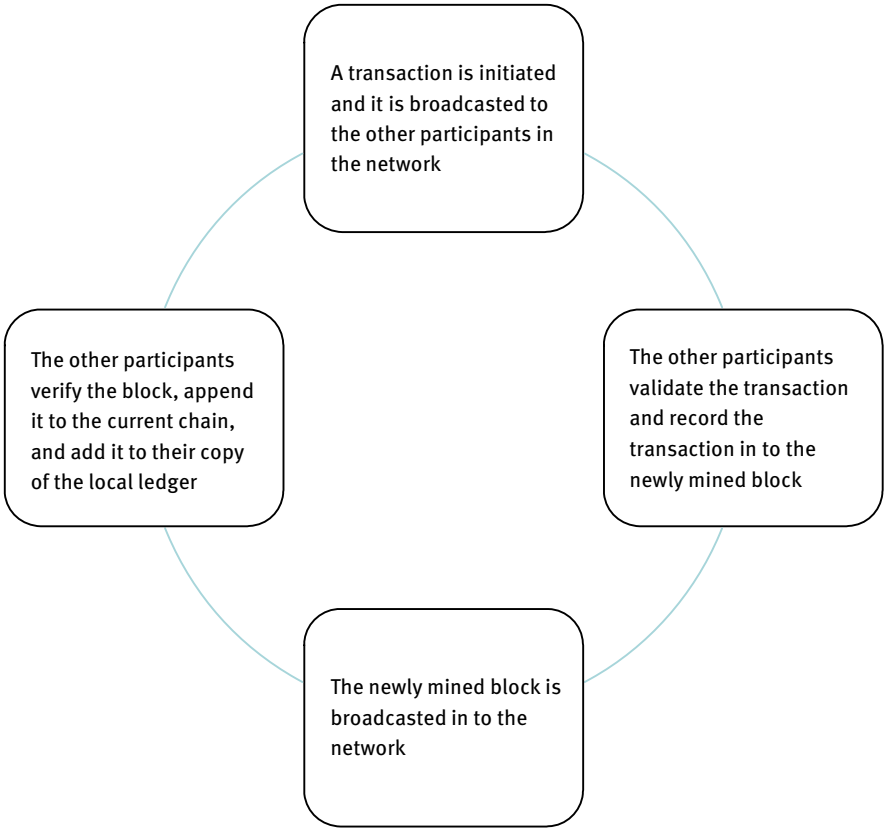

Fig. 4: The workflow of a blockchain

Firstly, a transaction is initiated by a participant and it is broadcasted to the other participants in the network. The participants who get this transaction use the digital signature to check the authentication of the transaction. After the verification, the transaction is attached to the list of authentic transactions in the participant's respective ledgers. To register the authentic transactions, the participants in the network work to mine the new block, i.e., finding the nonce of the block. Once a participant finds a valid nonce, they can mine the block that contains the concerned transaction. The other participants then check the trans-actions in the received block by analysing the Merkle root, and once the transactions in the newly mined block are authenticated and have not been tampered with, the new block is appended to the local replica of the blockchain. Once this entire procedure has been completed, the newly mined block can be appended to the current blockchain [21]. Sample code for blockchain as a service to declare the data of transactions and blockchain mining is given as below.

Listing 1: Blockchain as a service to declare the data of transactions and blockchain mining

```
#Transactions declaration
def get_transdata(self, sender, receiver, amount):
        self.current_data.append({
            'sender': sender,
            'receiver': receiver,
            'amount': amount
        })
        return True
#Blockchain mining
def blockchain_mining(self, details_miner):
            self.get_data(
            sender="0",
            receiver=details_miner,
            quantity=1,
        )
        last_block = self.latest_block
        last_proof_number = last_block.proof_number
        proof_number = self.proof_of_work(last_proof_number)
        last_hash = last_block.compute_hash
        block = self.build_block(proof_number, last_hash)
        return vars(block)
```

5.4 Features of blockchain

A few important features of the blockchain are listed below [22-25]:

- Decentralization: According to this feature, all the transactions are registered by all the participants in the network and each participant maintains a local copy of the ledger, where the recorded transactions are saved. In this way, the ledger is shielded from a central authority and a single point of failure.
- Trustable: According to this feature, the participants entering the network do not need to prove their identity as the participants need not depend on any particular participant for the validation of any transaction. There is no requirement of any third-party as the consensus algorithm is used for validating the transactions.
- Immutability: According to this feature, the transactions recorded into the blockchain can never be manipulated or tampered with. The cryptographic principles are utilized to make the blockchain and its contents immutable.
- Non-repudiation: According to this feature, no participant can deny making/receiving a transaction once the transaction is done. This is because every

transaction is cryptographically signed with a private key before broadcasting it to the network. This private key is known only to its owner, therefore making it impossible for an initiator to deny a transaction made by him/her.
- Transparency: According to this feature, every participant can access all the transactions recorded in the blockchain and verify all the transactions.
- Traceability: According to this feature, each transaction and block can be traced and verified easily with the help of the timestamp that is attached to the block header.

5.5 Potential attacks on blockchain

Like we know that every coin has two sides, even blockchain technology has certain vulnerabilities, leading to attacks on the blockchain. Some potential attacks are listed below:
- Sybil attack: An attacker floods the entire network with an enormous number of nodes with anonymous identities. In this way, the attacker can have control of a majority of the network and can try to dominate the network. Though the nodes seem to be unrelated, they are operated by a single partici-pant. This attack focuses on the entire network allowing the attacker to create a fork in the ledger making double-spending possible.
- Selfish mining attack: Generally, the longest chain in the network is con-sidered to be the true and latest version of the ledger. Therefore, if a selfish miner builds blocks on top of an existing chain in stealth mode, he/she will be able to publish this fake chain and everyone would accept this chain as it's the longest. This provides a small window to the attacker to perform double-spending.
- 51% attack: This attack occurs when a miner or a group of miners controls 51% or more of the mining power in a blockchain network. This is difficult to happen in large networks but it is highly possible in small networks.
- Denial of Service (DoS) attack: This happens when malicious participants completely absorb and keep the resources busy in verifying and transmitting the blocks and transactions. These malicious participants can flood the network with several transaction initiations to other participants, disabling the transmission and verification of transactions from other participants.

6 Cloud Security Concerns

The biggest problem today is the challenge to cloud protection. Malicious or unintentional acts can cause harm to an organisation at several levels. This is true in both cloud and non-cloud settings, but as the complexity of software and services

grows, security vulnerabilities also increase. The cloud attack surface is higher than the conventional service models, as the associated modules have several different endpoints and protocols to handle in different ways. A variety of methods are needed to recognise and resolve both identified and new threats.

Distributed-Denial-of-Service (DDoS) attacks are only one common security threat in cloud computing. Providers typically provide a variety of architectural solutions to configure a protected infrastructure to avoid these kinds of attacks, such as traffic separation (the ability to isolate clusters of virtual machines in groups of virtual different networks) or access control lists to establish guide-lines that specify multiple-level component permissions.

The second most significant problem for conventional cloud paradigms is Data Management. One part of data management that needs to be discussed is the consistency of the data. This means that all cloud users can see the same data simultaneously. This is no easy job, since hardware (data resources) are paired with the transactional status of operations in line with physical network constraints which can affect continuity by linking the user.

The third major concern is Resilience and Cloud compatibility. Resilience is the ability to manage errors gracefully and to restore the whole system. This is a massive problem for services and applications where modules fight for resources and depend on other internal or external components/services that malfunction or may rely on faulty software. Planning the manner in which those errors are observed, logged, repaired and restored re-quires not only developers but all teams as part of a cloud strategy.

To support, applications are available to replicate random problems, from hardware problems to major external threats, including failed implementations or suspicious device behaviour [26-27].

7 Blockchain to the Rescue

There are challenges and limitations in cloud computing apart from the ones that are mentioned above, some of these limitations can be removed or be mitigated using Blockchain Technology. The major challenges in cloud computing are security issues, cost management, lack of resources, governance or control of data, managing multiple clouds, building a private cloud, limited features, data mobility and a reliable internet connection.

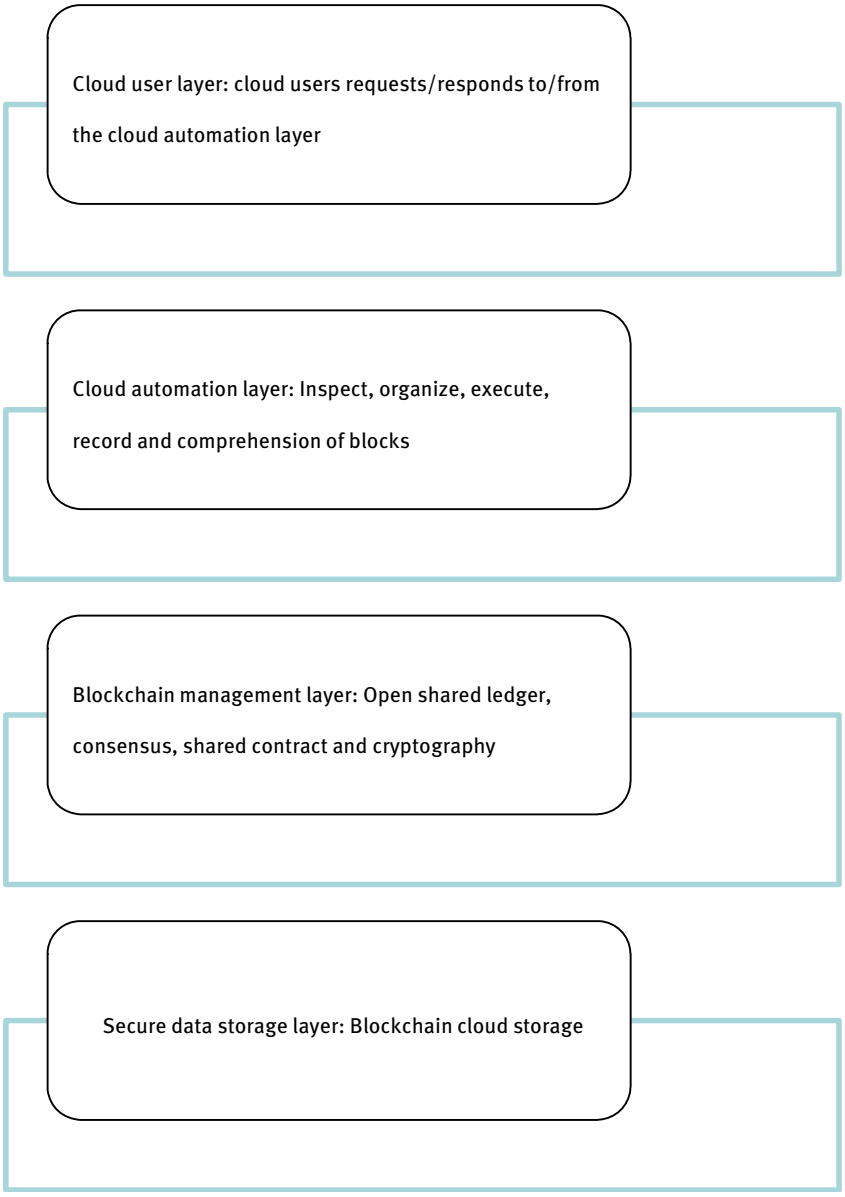

Fig. 5: Blockchain as a service (BaaS)

The major part of these problems can be resolved using blockchain technology. Blockchain as a service is shown in fig. 5. The characteristics of blockchain such as decentralization, Immutability, consensus mechanism, enhance security. The following problems can be solved using blockchain technology.

To solve security and privacy issues that are prevailing in cloud computing, blockchain uses secure exchange of transaction framework as shown in the fig. 6.

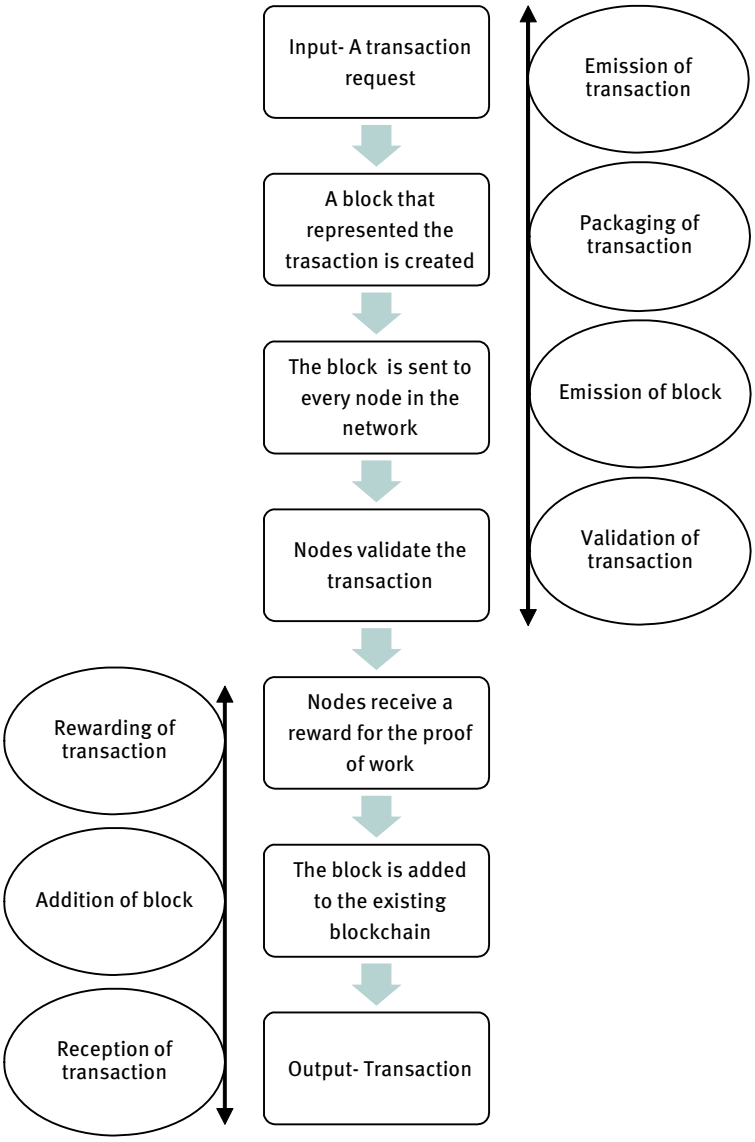

Fig. 6: Secure exchange of transaction framework in blockchain

7.1 Encryption

Although cloud services providers implement the best security standards and great certifications. Storing sensitive information will always come with the risk of malicious users and hackers trying to get the information. For example, the hacking of AWS EC2 console at Code Space, which led to data deletion and eventually the closing of the company. In Blockchain-as-a-Solution (BaaS), data is broken down into many encrypted segments, which are connected by a hashing feature.

These protected portions are split throughout the network and are decentralised in each segment. Security provisions are high such as account ledgers, public/private key encryption and haze blocks. It provides accurate and stable hacker protection. Due to sophisticated 256-bit encryption even experienced hackers cannot decrypt info.

7.2 Cost management

Maintaining a server or a database for storage is not cost effective, blockchain is decentralized which is secure and not in a single place or on a single server which reduces the cost by a marginal amount and it also decreases the storage needs for any firm. The security is not a problem as the blockchain has high security measures. As the load for retrieving any data is spread across multiple systems it is easier and faster to retrieve any files.

7.3 Lack of resources

There is a need for an expanding storage, in this scenario the use of blockchain is highly advantageous. We can use the concept of distributed ledger technology to distribute the load across multiple systems. If we are using a cloud or a centralized system it is costly to improve the speed of retrieving data.

7.4 Governance or control of data

There is lesser control of the transfer of data, it is difficult to keep track of who is accessing the data in a cloud environment whereas in the blockchain technology we can track each request and pull of data from the on-chain data or the data on the blockchain. Each query is stored on the blockchain as a transaction and it is irreversible. This makes it easier to grant permission for access of data and tracking of data queries is systematically filtered. Suppose there is a corruption of data on the chain, the system can be put offline and the copies of the data on the other blocks can be retrieved.

7.5 Managing multiple clouds or servers

With the ever increasing need to store any sort of data, we need an expanding storage. This is too costly to manage. The next solution is to manage multiple servers or cloud environments. This makes it really difficult to track and filter the data. In blockchain we can use multiple systems and solve this issue. We don't require multiple servers as the data on blockchain is stored in a decentralized manner.

7.6 Building a private cloud

If the data or any information is highly confidential then there is a need for a private cloud. This is not cost effective and costly; this can be solved using a private blockchain. Using a private blockchain has multiple advantages such as select granting of access and secure data transfer. Building a private blockchain is much easier than having a private cloud. Maintaining the storage modules and the server setup is a tedious and high maintenance work.

7.7 Limited features

Not all the cloud services were made with the same features. If there is a need for changing any characteristic on the cloud, migration of all the data is an extremely long and painstaking process. Using blockchain we can decide the initial set of characteristics and use them. As blockchain technology is constantly evolving the security measures and any other features can be updated whenever required.

7.8 Reliable internet connection

It is highly important to have a fast and strong connection using the internet or the intranet. The speed should be maintained from the retriever's side and the server-side. As the data is stored across multiple systems in a blockchain environment. A temporary downtime for a particular system will mean that the same data can be retrieved from a different block from the chain of blocks. This is one of the biggest problems in a cloud environment which can be solved using blockchain technology.

8 Conclusion

Cloud computing has given us multiple systems to store and manipulate data. We can definitely use blockchain to improve security systems and data sharing as compared to

the system that is present now. In this chapter, we addressed blockchain technology and associated key innovations and looked at the pattern of studies to date to explore more fields to be explored. Various existing concerns for the usage of blockchain in the cloud computing world should be taken into consideration. Blockchain is causing many problems right now, such as transaction stability, wallet, and applications, and multiple types of research have been conducted to fix the above-mentioned issues. The anonymous information of the user should be maintained in a secure manner by using blockchain in the cloud computing environment, and user information should be deleted when the user is withdrawing or discontinuing the usage of the service. If the information of the user is not discarded, it can be used to figure out who the user is and the identity of the user is exposed, the information retrieved can be used for malpractice.

Cloud infrastructure is here to remain, but be careful—Traditional methods will not be enough to solve the demands of current cloud workloads. Cloud storage, data management, and resource compatibility are real issues that need to be taken into consideration as part of a modern cloud strategy.

9 References

[1] Smith F, Waterman S, Identification of common molecular subsequences, J. Mol. Biol, 1981, 147, 195–197

[2] May P, Ehrlich H, Steinke T, ZIB structure prediction pipeline: composing a complex biological workflow through web services, Nagel W, Walter W, Lehner W, Euro-Par 2006 Parallel Processing, LNCS, 2006, vol. 4128, pp. 1148–1158, Springer, Heidelberg

[3] Toby V, Anthony V, Elsenpeter R, Cloud computing, A Practical Approach (1st. ed.), McGraw-Hill, Inc., USA, 2009

[4] Sabahi F, Cloud computing security threats and responses, 2011 IEEE 3rd International Conference on Communication Software and Networks, 2011, pp. 245-249, doi: 10.1109/ICCSN.2011.6014715

[5] Jin P, Jong P, Blockchain security in cloud computing: use cases, challenges, and solutions, Symmetry, 2017, 9, no. 8: 164

[6] Ravishankar B, Kulkarni P, Vishnudas M V, Blockchain-based database to ensure data integrity in cloud computing environments, 2020 International Conference on Mainstreaming Block Chain Implementation (ICOMBI), Bengaluru, India, 2020, pp. 1-4, doi: 10.23919/ICOMBI48604.2020.9203500

[7] Saurabh S, In-ho R, Weizhi M, Maninder K, Cho G, SH-BlockCC: A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology, International Journal of Distributed Sensor Networks, 2019, 15(4), 155014771984415, 10.1177/1550147719844159

[8] Yang X, Guojun W, Jidian Y, Ju R, Yaoxue Z, Cheng Z, Towards secure network computing services for lightweight clients using blockchain, Wireless Communications and Mobile Computing, 2018, 1-12, 10.1155/2018/2051693

[9] Hyun-Woo K, Young-Sik J, Secure authentication-management human-centric scheme for trusting personal resource information on mobile cloud computing with blockchain, Human-centric Computing and Information Sciences, 2018, 8 (1), 10.1186/s13673-018-0136-7

[10] Yue X, Wang H, Jin D, Mingqiang L, Jiang W, Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control, Journal of medical systems, 2016, 40(10),218, 10.1007/s10916-016-0574-6
[11] Simanta S, Application of blockchain in cloud computing, International Journal of Innovative Technology and Exploring Engineering (IJITEE), 2019, ISSN: 2278-3075, Volume-8 Issue-12
[12] Rajeswari S, Kalaiselvi R, Survey of data and storage security in cloud computing, 2017 IEEE International Conference on Circuits and Systems (ICCS), 2017, pp. 76-81, doi: 10.1109/ICCS1.2017.8325966
[13] Ashok G, Siddiqui S, Alam S, Mohammed S, Cloud computing security using blockchain, JETIR, 2019, Volume 6, Issue 6, 791-794
[14] Jadeja Y, Modi K, Cloud computing - concepts, architecture and challenges, 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET), Kumaracoil, 2012, pp. 877-880, doi: 10.1109/ICCEET.2012.6203873
[15] Gibson J, Rondeau R, Eveleigh D, Tan Q, Benefits and challenges of three cloud computing service models, 2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN), Sao Carlos, 2012, pp. 198-205, doi: 10.1109/CASoN.2012.6412402
[16] Kawanami Y, Kato H, Yamaguchi H, Tanimura M, Tagaya Y, Mechanism and control of cloud cavitation, J. Fluids Eng, Dec 1997, 119(4), 788-794 (7 pages), https://doi.org/10.1115/1.2819499
[17] Li X, Zhou L, Shi Y, Guo Y, A trusted computing environment model in cloud architecture, 2010 International Conference on Machine Learning and Cybernetics, Qingdao, China, 2010, pp. 2843-2848, doi: 10.1109/ICMLC.2010.5580769
[18] Liang Y, Blockchain for dynamic spectrum management, Dynamic Spectrum Management, Signals and Communication Technology, Springer, Singapore, 2020, pp 121-146, https://doi.org/10.1007/978-981-15-0776-2_5
[19] Nguyen C, Hoang D, Nguyen D, Niyato D, Nguyen H, Dutkiewicz E, Proof-of stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities, IEEE Access, 2019, 7, 85727–85745
[20] Liu Z, Luong N, Wang W, Niyato D, Wang P, Liang Y, Kim D, A survey on blockchain: a game theoretical perspective, IEEE Access, 2019, 7, 47615–47643
[21] Perboli G, Musso S, Rosano M, Blockchain in logistics and supply chain: a lean approach for designing real-world use cases, IEEE Access, 2018, 6, 62018–66202
[22] Konstantinidis I, Siaminos G, Timplalexis C, Zervas P, Peristeras V, Decker S, Blockchain for business applications: a systematic literature review, Abramowicz W, Paschke A, Business Information Systems, BIS 2018, Lecture Notes in Business Information Processing, 2018, vol 320, Springer, Cham, https://doi.org/10.1007/978-3-319-93931-5_28
[23] Umesh B, Sudeep T, Karan P, Pimal K, Sudhanshu T, Neeraj K, Mamoun A, Blockchain for Industry 4.0: a comprehensive review, 2020, IEEE Access, vol. 8, pp. 79764-79800, doi: 10.1109/ACCESS.2020.2988579
[24] Kshetri N, Can blockchain strengthen the internet of things?, IT Professional, 2017, vol. 19, no. 4, pp. 68-72, doi: 10.1109/MITP.2017.3051335
[25] Arora D, Gautham S, Gupta H, Bhushan B, Blockchain-based security solutions to preserve data privacy and integrity, 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), 2019, pp. 468-472, doi: 10.1109/ICCCIS48478.2019.8974503
[26] Houshyar H, Rashid M, Fakhrul A, Demidenko S, Multi-layer blockchain-based security architecture for internet of things, Sensors 2021, 2021, 21(3), 772, https://doi.org/10.3390/s21030772
[27] Rui Z, Rui X, Ling L, Security and privacy on blockchain, ACM Comput. Surv, 2019, 52, 3, Article 51, 34 pages, DOI:https://doi.org/10.1145/3316481

Sirisha Potluri, Sachi Nandan Mohanty, T. Kundana, D. Abhinav, P. Sushrutha

Security and Privacy Preservation Model to Mitigate DDoS Attacks in Cloud

Abstract: Denial-of-service (DoS) attack occurrences are among the key security challenges within the rising cloud computing models. Currently, a number of different types of DoS attacks are conducted against the various cloud services and resources, which target their availability, service level agreements SLAs, and performance. A successful DDoS attack would possibly lead to service degradation or complete outage. DDoS attacks will reduce the network re-sources which may result in bandwidth depletion. The main objective of DDoS attacks is to prevent certain users from accessing the services in the cloud. In this research, we propose a privacy-preserving cross-domain at-tacks detection scheme for SDNs. Predis may be a combination of perturbation encryption and encoding to guard the privacy and uses a computationally simple and efficient machine learning algorithm k-Nearest Neighbour (KNN) for its detection. Here we also improve the KNN to achieve much better efficiency. Through extensive simulations and theoretical analysis. The DEMO of this algorithm is capable to realize the detection process efficient and accurate attack detection by keeping sensitive information secure. Virtualization enables simultaneous sharing of resources from a single server to some applications or services, this induces a certain amount of threats and security issues for the cloud. This module focuses on identifying challenges related to cloud security and tries to introduce ways in resolving these issues

Keywords: Denial-of-Service, KNN, Software Defined Networks, Cryptography, Virtualization, Cloud Security, Cloud Privacy

Sirisha Potluri, Department of CSE, IcfaiTech (Faculty of Science and Technology), ICFAI Foundation for Higher Education, Donthanapally, Shankarpalli Road, Hyderabad, Telangana 501203, India, sirisha.vegunta@gmail.com
Sachi Nandan Mohanty, Department of Computer Engineering, College of Engineering Pune, Wellesley Rd, Shivajinagar, Pune, Maharashtra 411005, India, sachinandan09@gmail.com
T. Kundana, Department of CSE, IcfaiTech (Faculty of Science and Technology), ICFAI Foundation for Higher Education, Donthanapally, Shankarapalli Road, Hyderabad, Telangana 501203, India, kundana666666@gmail.com
D. Abhinav, Department of CSE, IcfaiTech (Faculty of Science and Technology), ICFAI Foundation for Higher Education, Donthanapally, Shankarapalli Road, Hyderabad, Telangana 501203, India, dabhinavriser@gmail.com
P. Sushrutha, Department of CSE, IcfaiTech (Faculty of Science and Technology), ICFAI Foundation for Higher Education, Donthanapally, Shankarapalli Road, Hyderabad, Telangana 501203, India, psushrutha15@gmail.com

https://doi.org/10.1515/9783110732573-003

1 Introduction

The practice of employing a network of remote servers hosted on the web to store, manage, and process data, instead of a local server or a private computer is called cloud computing. It is a pay-for-use model. Cloud computing can be considered as the future of the emerging technologies because of the combination of emerging technologies like virtualization and service oriented architecture. Based on the deployment models there are various types of clouds [1].

- Public/Internet Cloud
- Private/Enterprise Cloud
- Hybrid/Mixed Cloud
- Community Cloud

Public cloud is designed for a substantial set of public clients, Private clouds services are available only for the cloud owners. The combination of two or more clouds can be considered as hybrid cloud where in the two clouds can be either public or community or private clouds, broadly community clouds services are shared between several organizations.

Cloud provides services using various models like Software as a Service, Platform as a Service and Infrastructure as a Service.

- SaaS: It provides user access to software applications. These software applications which are present in the cloud are used for an enormous range of tasks.
- PaaS: It provides all the hardware and software components that are required to build cloud-based applications.
- IaaS: It dispenses services like storage, security tools, and networking for end users.

Several critical security attacks are designed and proposed against various cloud deployment models which pose severe security risks to the adaptor. Attacks such as wrapping, malware injection, and other attacks can be conducted against cloud computing. One such security attack is the Denial of Service (DoS) attack. It is an event or malicious behaviour that mitigates or prevents the cloud's security to perform its expected functions and services. A distributed form of DoS attack is called a Distributed Denial of Service (DDoS) attack which applies numerous network hosts to inflict more effects on the dupe [2].

DDoS attacks can be classified into the subsequent categories

- Attacks on Bandwidth
- Physical Disruption.
- Limitation Exploitation
- Attacks on Connectivity
- Exhaustion of Resources
- Process disruption
- Data corruption

Software-Defined Networks (SDNs) have emerged as a new communication paradigm, released from direct integration into traditional networks and provides a system and network flexibility through a sensible network controller. SDNs contain a data plane, a control plane, and an application plane. The control plane contains some controllers that use the logic control strategy and maintain the entire network view as logic-centric. Administrators remove all network views from network services and provide an easy-to-use interface for providers, researchers, or third parties to facilitate these employees to customize transaction plans and see reasonable network management. SDNs users do not have to worry about the technical details of the device below, a simple system can detect the fast delivery of new applications

Advanced control features and systems enable SDNs to be exposed to known as Distributed Denial-of-Service (DDoS) attacks. For example, the controller, which plays a very important role in determining the performance of each component in SDNs, is the main target of DDoS attacks. A compromised controller can lead to the misconduct of all the switches under their control. Denial of service (DoS) attacks can run out of system resources on a targeted computer, stop services, and leave its normal users inaccessible. When hackers use two or more compromised computers as a "doll machine" to launch a DDoS attack on a particular target, it is called a DDoS attack. The IP address of the grinding machine and the composition and type of attack package are not set, making it difficult to locate the attacker.

DDoS attacks have become a major threat to the Internet today and attacks make online services unavailable to large victims on the road from multiple attackers. With the number of businesses offering their services online growing exponentially, a DDoS attack could lead to significant financial losses. A recent report reveals that DDoS is attacking a 22% data recovery account for 2015 [3-4].

DDoS attacks work in three steps, namely scanning, logging in, and launching attacks. The unusual mobility of DDoS attacks often affects multiple paths and network domains. The paper also deals majorly with KNN models which will be improvised to detect attacks.

Cloud computing is one form of distributed system containing a set of virtual machines that can be dynamically provisioned to meet the changing requirements of resources by the customer. The cloud-customer relationship is governed by the service level agreement (SLA).

Overhead of physical installation and maintenance of such a huge system issue is relieved by the cloud thus reducing the overall costs and also increases efficiency. Virtualization in cloud computing assumes Service-Oriented Architecture (SOA) that enables the transformation of customer requirement problems into services thus benefitting the idea of cloud computing. The cloud customer has to depend on the Cloud Service Provider (CSP) for security and privacy of their information.

Therefore, clearly there should be goals for the information security that should be satisfied which are:

C – Confidentiality
I – Integrity
A – Availability

Confidentiality means making sure that the information that has to be kept secured is secured and there shall be no access for unauthorized users to read the information. Integrity means making sure that unauthorized users cannot modify or destroy the information. Availability means making sure that authorized people are not prevented from accessing the information.

Cloud architecture and its disparity from standardized traditional onsite system makes the identification and separation of different aspects in cloud security an arduous task.

This module is an attempt in exploring various security challenges and proposing suitable solutions for cloud security.

2 Literature Analysis

In the DDoS attacks, the attacker dispatches an order to a system called as command and control server (C&C server) which will coordinate and trigger a botnet. Generally, a botnet can be considered as a set of compromised hosts, which obscure the attacker by providing a level of indirection. The C&C server orders the botnet to launch a DDoS attack against the victim (server), and afterward, the bots will direct the attack packets to the victim whose content depends on the type of attack. Thus, the attacker host is separated from its victim by one or by tons of intermediate layers of zombie hosts. A zombie or bot is a compromised computer under the control of an attacker who controls many other machines which altogether form a botnet [5-7].

3 Classification of DDoS Attacks

Distributed denial-of-service attacks can be categorized based upon on its various features and origin of an attack. DDoS attacks can be categorized as external DDoS attacks and internal DDoS attacks [8-10].

3.1 Various types of external and internal attacks

3.1.1 External attacks to internal attacks

In this case, the botnet which performs the attack comes from an exterior target system. The attack can target a net entrée of the Cloud infrastructure or the servers. If a specific client in a virtual machine becomes a victim of an attack, it'll also affect the opposite virtual machines present on the equivalent server of the Cloud.

3.1.2 Internal attacks to external attacks

In this case, the attack can tackle by taking possession of a virtual machine that is running within the Cloud. This can be done with a Trojan horse. A Trojan horse is malicious software or a code that can take control of the system. The choice of which depends on the customer's virtual machine to infect is important because if a customer owns a large number of virtual machines, the Trojan horse can probably spread all over the virtual machines, thus forming a botnet.

3.1.3 Internal attacks to internal attacks

In the Cloud infrastructure, an internal botnet is formed which can attack another target inside the system such as a single virtual machine or a bunch of virtual machines. All the Cloud infrastructures may break down under these kinds of attacks. Different kinds of attacks approach different types of attackers where each type of attack scenario correlates to a particular attacker with a specific location and goals.

3.2 Classifications of DDoS attacks

3.2.1 Protocol vulnerability exploitation

These attacks take advantage of the known weaknesses which are present in the protocol such as flaws in design or implementation of triggers, inappropriate activities, and can change the data that goes to and from a particular goal. Depending on the design certain protocol steps might be created to check the potential for DoS attacks.

3.2.2 Malformed packets

A malformed packet attack are often launched against many protocols. For instance malformed packet attack against IP protocol. In IP packet options attacks, malformed packets can randomize the optional fields which are within an IP packet and can set all the standard of service bits to at least one, which could cause more processing within the victim for packet handling

3.2.3 Flooding attacks

Flooding attack is also called Bandwidth distributed Dos (BW-DDoS), the attacker tries to flood the victim with unwanted traffic to prevent legitimate traffic. Based on the type of protocol flooding attacks differs. Few of the strong attacking agents include privileged zombie which has control over its host whereas weak agents include programs that are downloaded automatically and run in sandboxes.

3.2.4 Amplification attacks

They are the devastating version of reflective DDoS attacks. They utilize the inherited nature of network protocols to increase the amount of traffic that is reflected in the victim. As a result, the traffic that reaches the victim is amplified by the reflector server. Amplification DDoS attacks are created by the amplification through flow multiplication attacks or through payload magnification where a large number of responses are reproduced or response messages bigger than the corresponding requests are issued by the reflector

3.2.5 Reflective attacks

Another method that's applied by the DDoS attackers is the reflective method. This method helps the attacker to send traffic to the victim indirectly and helps the attacker to stay undetected. During this method, all attack packets, which the attacker sends contain the IP address of the victim within the source address field of IP packets.

Classification of DDoS attacks is given fig. 1.

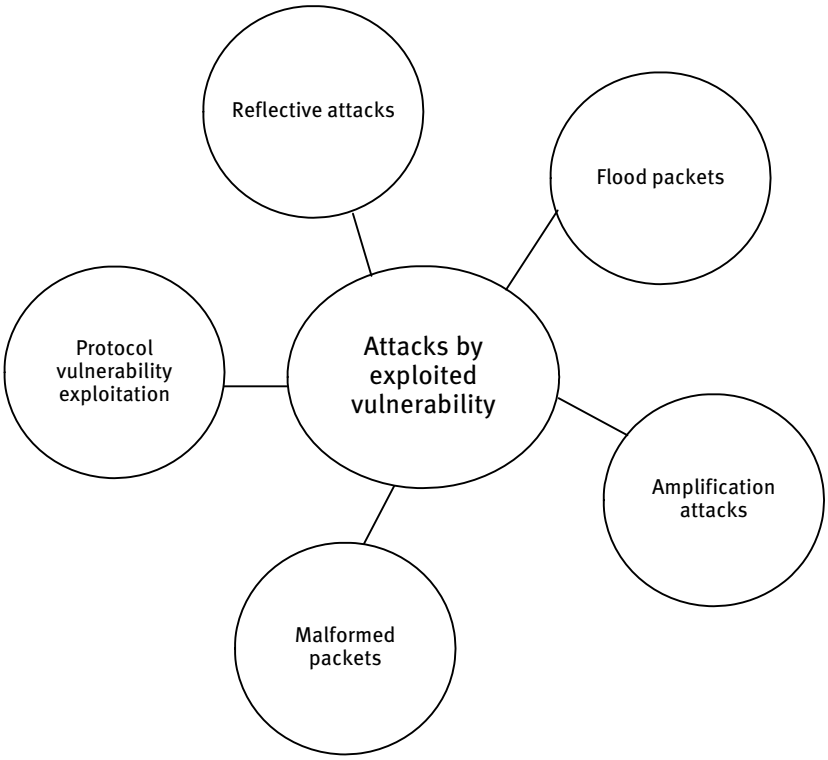

Fig. 1: Classification of DDoS Attacks

3.3 Current popular DDoS attacks

- AgoBot: It is one among the foremost popular bots with an anti-virus vendor that has over 600 versions. Its variants are Gaobot, Nortonbot, Phatbot, and Polybot
- SDBot: It's over 1800 variants and comes with ping and UDP flooding tools.
- RBot: It has over 1600 variants and is written in C++ to focus on windows system.
- SpyBot: It's written within the C programming language and also affects the windows operating system.

3.4 Factors effecting severity of DDoS attacks

- Type of attack
- Type of protocol or event misused within the attack
- No: of attacking hosts
- Amount of resources at the victim's site
- Type of cloud, mostly public cloud

4 DDoS Mitigation Techniques

DDoS mitigation techniques help us in effectively combating the attacks. Few of the mitigation techniques are as follows:

4.1 Reducing attack surface

Reducing the services which will be attacked limits the choices for attackers. Using Firewalls and Network Access Control Lists will allow only necessary traffic, to necessary ports from essential hosts only. Considering the case of web servers, they permit traffic from anywhere to port 80 of your webserver. And in such cases, one should further take other protective measures. Even for the websites which are accessible across the web, one can reduce the area by restricting traffic to countries where users are located.

4.2 CDN's

CDN'S distributes the content and boosts the performance by minimizing the space between resources and between the end-users. It stores the cached version of the content in multiple locations and this eventually mitigates DDoS attacks by avoiding one point of failure, when the attacker is trying to pivot on a single target.

4.3 Black hole routing

As the name propounds, black hole routing, with none of the filtering routes both legitimate and malicious traffic route to a null route or black hole where the traffic will be dropped from the network. Depending on the pattern, if one can identify the attacker, then the packets are often filtered and can be routed back to the black hole.

5 Stages of DDoS Mitigation

5.1 Detection

Initially there is a need to detect if an attack is present or not. At this phase, there is a need to identify the legitimate traffic and malicious software. In the event of mitigating DDoS one shouldn't drop potential customer traffic which would be disastrous.

5.2 Response

Once the attack is detected now there is a necessity to seek out how to respond to those attacks.

5.3 Routing

By intelligent routing, one can break the remaining traffic into manageable chunks which will be handled by cluster resources to which it's being routed.

5.4 Adaption

This is the of the foremost important stage of DDoS mitigation where one has got to search for patterns of DDoS attacks and check if this analysis can further strengthen the mitigation techniques.

6 Privacy in DDoS Attacks

ANALYSIS OF DATASET LLDOS is as follows:

Stage Flow Number	172.16.112.* 172.16.113.* 172.16.114.* 172.16.115. *
Victim Attacker Combine Scanning	424 328 32 296 0 1081 1081
Intrusion	128 0 97 0 0 332 335
Attacking	2 0 0 285 107465 199 107667

The KNN features for ease of use are very useful for us when we want to embed other special functions in the separator to protect the privacy of test data. On the other hand, KNN, as a partitioning algorithm, works well with precision, and KNN is not sensitive to vendors who can maintain high accuracy when there are certain sounds in the database.

The European vector n dimensional formula is:

$$d = \sqrt{\sum_{i=1}^{n}(X_{i1} - X_{i2}) * 2} \tag{1}$$

KNN as high precision is widely used in a lot of different areas.

7 Summary of Our Contributions Using KNN

- We recommend Predis, a DDoS privacy protection program for SDNs privacy, which looks at both the detection of DDoS attacks and privacy protection in multi-party partnerships. Predis uses SDN features and an improved KNN algorithm to detect DDoS attacks accurately during real-time and integrates digital cryptography and perturbation encryption to provide each participant's privacy and confidentiality.
- We attest to Predis's security in the asymptotic form of computer security in modern cryptography. By strict security analysis, we confirm that the traffic data provided by each participant is inseparable from its potential adversary.
- We do extensive research using the most authoritative data sets to show that Predis is timely and accurate. We show that our system can not only determine if traffic is normal, but can also detect unusual traffic at the beginning of a DDoS attack. The results show that Predis is more accurate than the existing adoption schemes, which currently protect participant's privacy. A detection attempt restricted within one domain would be unable to spot the attacks at their primary stages. Thus, the involvement of multiple domains in attack detection will help to realize more accurate and timely detections.

8 Summary of DDoS Attacks Detection Methods

There are no. studies on DDoS attack detection because of the prevalence and severity of DDoS attacks. So we briefly summarize related work from 2 perspectives, i.e.- DDoS attacks detection in conventional networks and DDoS attacks detection in SDNs. Detection approaches of DDoS attacks have been researched exceedingly in conventional network models [11-12].

8.1 Conventional network entropy

- Support Vector Machine
- Naive Bayesian
- Neural Network
- Cluster Analysis
- Artificial Neural Network
- K-Nearest Neighbours

8.2 SDNs

- Self- organizing map B
- Support Vector Machine
- Entropy variation of the destination IP address
- Deep Learning
- Bayesian Networks

The attackers of DDoS can simultaneously control several computers and make an attack architecture that contains control puppets/dummies and attack puppets/dummies in the computing environment. The traditional attack architecture is analogous to the dumbbell shape structure. Wherein an intermediate network is mainly responsible for data forwarding, security events and control functions are done by the management, while the network itself can't detect network attacks and deal with them.

9 Privacy Preserving in Cross-Domain Detection

A SDNs domain in Predis refers to the controlled domain which is under SDNs architecture, which is in the network domain along with deployment of the SDNs techniques and can independently get controlled by operators. The SDNs domains conduct a centralized way of controlling data forwarding. The multiple SDNs domains explain in our paper collaborate and these SDNs domains may or may not be adjacent to each other physically or in geographical location. Control plane of this domain sends the flow table to a selected location on the computing server. The computing server provides the DDOS detection service and returns detected results to controllers.

The traditional network domain for traffic forwarding is a distributed control where it cannot achieve centralized control. Privacy-preserving cross-domain attacks detection are often seen as a Secure Multiparty Computation (SMC) problem, which is that the matter of the way to calculate a function safely when no credible third party is present there [13-14].

KNN algorithm occurs in embedding encryption steps. After providing training details, KNN can separate test samples by selecting a distance measurement formula outside the training phase (Euclidean grade selected in Predis).

10 Models

10.1 System model/approaches and threat model

We first go through the overview of the system model/approaches and the roles included in Predis. Then we present the threat model, followed by security.

It has three sorts of roles:

- Server for Computation (CS)
- Server for Detection (DS)
- Software Defined Networks SDNs domain 3

Domain D n is the nth domain that participates in the attack detection and provides the data to CS and DS. Which in turn, provides computing & encryption services for domain Dn. Each domain sends traffic information to CS for the calculation purpose and receives the detection results from DS. CS provides computational service and sends the intermediate results to DS. Where this later provides detection service based on intermediate results and replies to the detection results of each domain. Thus, CS and DS perform computation in collaboration with each other. Predis provides accurate DDoS attacks detection service for domains wherein each domain is not willing to share privacy traffic information.

Here, we provides a formal definition of privacy. The knowledge of the flow table is provided by domains that participate within the detection is called privacy. Importantly, privacy includes IP Source, IP Destination, Port Source, Port Destination, Length, and Flow Packets. The basic operations includes these three roles mentioned earlier as functions with input and output. Each function is meant to run on continuous inputs in real-time data partitioned into a particular interval and Predis features a set of n input peers with it. Sample code of DDoS is given as below.

Listing 1: Performing DDoS attack for service inaccessibility

```
import socket
import sys as s1
import os
print("DDoS Attacking: "+s1.argv[1]+" Initiating...")
print("Inject Code "+s1.argv[2])
def attackFunc():
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.connect((s1.argv[1], 80))
    print(">>> GET Message /" + s1.argv[2] + " HTTP/1.1\n")
    s.send("GET Message /" + s1.argv[2] + " HTTP/1.1\n")
    s.send("From Host Initiate: " + s1.argv[1]  + "\n");
```

```
    s.close()
for var in range(1, 10000):
    attackFunc()
```

11 Security in Different Cloud Computing Service Models

Three service models of cloud that provide services at different layer are Software as a service, Platform as a service and Infrastructure as a service respectively.

SaaS – Customer has minimum command on security as the backend infrastructure and also the platform of execution is present outside the range of the customer. PaaS – In PaaS, the customers have a certain amount of command on the deployed applications and remotely on configuration settings for the application environment. This framework gives more control over security compared to SaaS but less control than what IaaS gives. IaaS – In IaaS, the customer has much more control over security than the two other models as IaaS delivers virtual computing resources as networking, storage devices, and hardware.

12 Security in Different Cloud Deployment Models

The four deployment models of cloud out of which the customer selects based on suitability, requirement, and purpose of the user cloud are Public, Private, Community Cloud, and Hybrid clouds.

Public Cloud – Organizations have to compromise certain aspects of security in this deployment model as the cloud lies at the service provider end. Customers are unaware of the geographical location of their data, type of storage used by CSP hence making this model a bit less secure.

Private Cloud – It is owned by a single organization or by an on or off-premise located the third party. This deployment model solves a few aspects of security issues faced in the public cloud to some extent but has its difficulties like provisioning, storage management, and capacity watching.

Community Cloud – It is owned by a community of organizations that have a common interest. The drawback of this model is that there are several unanswered questions in terms of data proliferating across multiple domains and organizations and service outrages.

Hybrid Cloud - As a hybrid cloud is a combination of any of the two deployment models, it covers the benefit of scaling, cost, and also the security. Data privacy and integrity form a threat in the hybrid model.

13 Vulnerabilities in Cloud

Virtualization is the backbone to cloud and it comes in three levels. First at the operating system level, second at application level and finally at hypervisor level.

In the operating system level, multiple guest operating systems run on the host operating system making guest operating systems vulnerable as the control is at the host operating system. If the host OS is compromised, then so is the guest OS.

The application level is located just above the host OS layer. Hence the virtual machines which run guest OS along with its subsequent applications also suffer from the same vulnerability which is present at the operating system level.

At the hypervisor level, as the virtual monitor (VMM) or the hypervisor which is a software layer runs on the host operating system, every other virtual machine which runs on guest operating systems are controlled by the hypervisor at host OS making it a vulnerable case because when hypervisor at host OS is compromised, then so are virtual machines at guest OS. A small flaw at the hypervisor level creates risk for the entire infrastructure of the cloud; also the breaches in hypervisor create cross virtual machine attacks.

Since the cloud services are acquired by its users through the application interfaces (APIs) provided by cloud service providers, we can say that the security of these APIs directly affects the security of the cloud. Loopholes in TCP/IP protocol explicitly cause vulnerabilities typically to public clouds

13.1 Threats

As the computing infrastructure of the cloud is present off-premises, the organization or the users who have opted for the cloud services must assess the risk involved when there is a loss of control of these services.

In the beginning stages of users acquiring the cloud services, there is a chance that with insufficient knowledge, they can set the whole infrastructure of cloud at risk by improper usage of storage capabilities, processing, and by the deployment of dubious applications. This kind of threat is highly relatable to PaaS and IaaS.

Also by knowing the entire or part of the system, an attacker knows how to go through security mechanisms. The attacker also can have privileges to bypass firewalls and also for intrusion detection systems. Virtualization, sharing of resources, and multi-tenancy are the concepts that also help the attacker in exploiting the loopholes and give the ability to manipulate the service models.

The data in cloud services traverse across the continents where there is a chance for issues arising in terms of jurisdiction as different geographic locations have different obligations in laws than the service provider.

Deceptive mechanisms and weak passwords may lead to the user being the sufferer of identity theft.

An attacker can launch denial of service attacks by flooding the users with requests, can attack virtualization using hypervisor root kits, can do phishing, and can do meta-data spoofing with the above-mentioned vulnerabilities and threats.

14 Security Issues

14.1 Security issues layer-wise

Cloud can be viewed in distinct layers such as a physical, Virtualization, Service provider and User layer. There are certain security issues associated with each layer.

Tab. 1: Security issues in cloud computing architecture layer-wise

Layer	Description	Security issues
Physical layer	Provides computing, storage, and networking resources.	1. Database intrusions 2. Data storage issues 3. Confidentiality, integrity, availability. 4. Network vulnerabilities and attacks
Virtualization layer	The hypervisor is present at this layer along with the guest operating systems and virtual machines	1. Access control issues 2. Regulations compliance 3. Hypervisor and virtual machines exposure 4. Isolation between virtual machines
Service provider layer	Offers management services such as scheduling, load balancing, accounting policy management, resources provisioning, and monitoring.	1. Trust management 2. Transient data security issues 3. Authentication and authorization issues 4. Audit, regulations compliance 5. Policy enforcing
User layer	Have applications, application interfaces, and tools.	1. Authentication, access control 2. Exposure of browser and API's 3. Vulnerabilities in applications

15 Proposed Solutions in Literature

Various state of the art methods in literature are listed as follows.

15.1 Data confidentiality schemes

Tab. 2: Data confidentiality schemes

Name of the scheme	Proposed by	Idea of the scheme	Algorithms used
Searchable Encryption	I-En Liao & Jyun-yao Hung (2012)	Secret sharing and searchable encryption	1. Non-numeric file search 2. Data Encryption
Onion Encryption	Curino et al. (2011)	Adaptable security providing different layers of encryption in order to maintain the confidentiality of the user data	1. Query Execution 2. Data Encryption
Fully Homomorphic Encryption	Tebba et al. (2012)	Allowing the clients in encrypting their data before storing at cloud service provider there-by ensuring the data confidentiality	1. Encryption 2. Key - Generation 3. Evaluation
Encryption for secure scalable fine grained access control based on attributes	Yu et al. (2010)	To Protect user data by using cryptographic techniques and also to induce overheads of key distribution and management on the client data.	1. Key - Generation 2. Setup 3. Encryption 4. Proxy Re 5. Decryption

15.2 Cloud virtualization confidentiality schemes

Tab. 3: Cloud virtualization confidentiality schemes

Name Of The Scheme	Proposed By	Idea of the Scheme	Algorithms Used
PALM	Zhang et al. (2008)	Prototype that ensures security of protected user data and backup data while and after	1. Metadata Migration Protection 2. Migration data Protection

Name Of The Scheme	Proposed By	Idea of the Scheme	Algorithms Used
		VM live migration	
Trusted cloud computing platform (TCCP)	Santos, Gumadi and Rodrigues (2009)	Targets at preserving confidential execution of VM's	1. VM Launch 2. Node Registration
Self-service cloud computing scheme (SSC)	Ganapathy V (2015)	To solve the issues related to uninterrupted cloud service provider access on the client CPU contents, memory and registers.	1. Create_MTSD 2. Create_UDom() 3. Create_Userdomain 4. Bootstrapping_SSL 5. Grant_Privilege
TVDC	IBM (2008)	Concept in which each VM is restricted from accessing any other VM thus ensuring protection from unwanted data leakage	1. Authorization of VMM 2. Resource Access 3. Infrastructure Integrity and Network Isolation 4. Inter VM communication

15.3 Cloud data integrity schemes

Tab. 4: Cloud data integrity schemes

Name of the scheme	Proposed by	Idea of the scheme	Algorithms used
Public verifiability and data dynamics scheme	Wang et al. (2009)	To provide cloud data storage integrity	1. KeyGen 2. SigGen 3. GenProof 4. VerifyProof 5. ExecUpdate 6. VerifyUpdate
MHT	Niaz M.S, Saake Gin (2015)	Merkle's scheme for maintaining user data integrity without the overhead of maintaining a table at owner side of data.	1. Multi-Join 2. Single-Join 3. Zero-Join 4. Range Condition
Dynamic provable data possession	Erway et al. (2009)	Supports data spontaneity with cloud data integrity	1. Prepare Update 2. Verify Update 3. Perform Update 4. Challenge 5. Proof 6. Verify

Name of the scheme	Proposed by	Idea of the scheme	Algorithms used
Privacy preserving public auditing scheme	Wang et al. (2015)	To assure data integrity of cloud storage and providing an optimal data verification methodology to prevent integrity breaches	1. KeyGen 2. SigGen 3. GenProof 4. VerifyProof

15.4 Integrity schemes in cloud virtualization

Tab. 5: Integrity schemes in cloud virtualization

Name of the scheme	Hypervisor used	Algorithms used
ACPS	KVM	1. Checking Activity 2. Logging of Activity 3. Checksum calculation 4. Alert Generation 5. Generating Security Response
SSC	XEN	1. Create_UDom
MIRAGE	VMware	1. Access Control 2. Image Transformation 3. Provenance Tracking 4. Image Maintenance
PALM	Xen	1. Data Protection Migration 2. Metadata Migration Protection

16 Onion Encryption (OE)

This is a data confidentiality scheme. It is an outlook to an adaptable security with distinct layers of Encryption (similar to layers of an onion) so that the SQL queries can be executed on the encoded data which includes aggregates, operations of ordering. joins and the processing of query is done at the cloud service provider's end simultaneously maintaining user data secrecy as decryption will happen at the client end.

The primary focus is to maintain distinct levels of encryption for every column and decoding every column as per the requested query.

This scheme uses two algorithms

– Data Encryption Algorithm
– Query Execution Algorithm

These algorithms take the use of keys such as RND, DET, OPE, HOM.

1. Randomized Encryption Key (RND): It provides similarity under an adaptive chosen plain text attack.
2. Order preserving Encryption Key (OPE): For the queries which involve choices based on comparison, this key provides secured execution.
3. Homomorphic Encryption Key (HOM): For the queries which involve server side aggregates calculation, this key is used for execution.
4. Deterministic Encryption Key (DET): Queries which involve a selection on equality for a specific value, this key is used for execution.

Time complexity: Time complexity can be calculated as

If T1 = time spent in redrafting queries

T2 = Time required in encoding and decoding payloads

Time complexity is the order of T1 * T2 i.e., O (T1*T2)

It has been discovered that onion encryption scheme brings a comprehensive drop in throughput by 22.5%.

17 Conclusion

Cloud computing comes with known vulnerabilities because of the combination of technologies like network links, web servers, virtual machines, etc., since cloud computing has an advantage of scalability and elasticity it offers adequate resistance to attacks. Among those, the DoS and DDoS are easy to escalate and are more destructive. Security should be considered as shared responsibilities of both cloud providers and users. Traditional computing has been completely transformed to a cost effective, optimized computing by cloud computing. Yet there are some challenges and issues in regard with secured information sharing in cloud. Existing security measures needed to be enhanced and also new security mechanisms are needed in order to eradicate security issues in cloud environment.

In this paper few of the mitigation techniques, solutions, and schemas are presented through which the security and privacy of the cloud can be preserved. Few of the solutions could not perfectly mitigate all the possible attacks, but other solutions are efficient. An SDN-based cross-domain attacks detection scheme was presented that provides privacy protection. Also, we came across cross-domain privacy protection problems and also the DDoS attacks detection based on SDNs, in which we combined geometric transformation and data encryption methods in the intention to protect privacies, broke down the detection process into two steps, disturbance, and detection, which involved two of the servers that work together to complete the detection process by using the concept of cloud virtualization. An

enhanced KNN algorithm for low time consumption and high accuracy was represented. Extensively experiment of different authors results showed that Predis is proficient in detecting cross-domain anomalies while preserving privacy with the best time complexity and high accuracy. The overall paper can be used to further reduce the time consumption of Predis in attack detection in the future.

18 References

[1] Saurabh S, Young-Sik J, Hyuk J, A survey on cloud computing security: issues, threats, and solutions, journal of network and computer applications, 2016, Volume 75, Pages 200-222, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2016.09.002

[2] Shankarwar M, Pawar A, Security and privacy in cloud computing: a survey, Satapathy S, Biswal B, Udgata S, Mandal J, Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014, Advances in Intelligent Systems and Computing, 2014, vol 328, Springer, Cham. https://doi.org/10.1007/978-3-319-12012-6_1

[3] Andrew C, Mohammad H, Omar A, Defence for distributed denial of service attacks in cloud computing, Procedia computer science, 2015, Volume 73, Pages 490-497, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2015.12.037

[4] Mohammad M, Marzie J, A survey and taxonomy of DoS attacks in cloud computing, Sec. and Commun. Netw, 2016, 9, 16, 3724–3751, DOI:https://doi.org/10.1002/sec.1539

[5] Potluri S, Mangla M, Satpathy S, Mohanty S N, Detection and prevention mechanisms for DDoS attack in cloud computing environment, 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2020, pp. 1-6, doi: 10.1109/ICCCNT49239.2020.9225396

[6] Priyanka K, Munesh T, Virendra Y, Vikash S, Detection techniques of DDoS attacks: a survey, 2017 4th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics (UPCON), Mathura, India, 2017, pp. 675-679, doi: 10.1109/UPCON.2017.8251130

[7] Zhang P, Huang X, Sun X, Wang H, Ma Y, Privacy-preserving anomaly detection across multi-domain networks, 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery, Chongqing, China, 2012, pp. 1066-1070, doi: 10.1109/FSKD.2012.6234272

[8] Jelena M, Peter R, A taxonomy of DDoS attack and DDoS defense mechanisms, SIGCOMM Comput. Commun, 2004, Rev. 34, 2, 39–53, DOI:https://doi.org/10.1145/997150.997156

[9] Soule A, Ringberg H, Silveira F, Rexford J, Diot C, Detectability of traffic anomalies in two adjacent networks, Uhlig S, Papagiannaki K, Bonaventure O, Passive and Active Network Measurement, PAM 2007, Lecture Notes in Computer Science, 2007, vol 4427, Springer, Berlin, Heidelberg, https://doi.org/10.1007/978-3-540-71617-4_3

[10] Yaar A, Perrig A, Song D, Pi: A path identification mechanism to defend against DDoS attacks, 2003 Symposium on Security and Privacy, 2003, Berkeley, CA, USA, pp. 93-107, doi: 10.1109/SECPRI.2003.1199330

[11] Shui Y, Yonghong T, Song G, Dapeng W, Can we beat DDoS attacks in clouds?, IEEE Transactions on Parallel and Distributed Systems, 2014, vol. 25, no. 9, pp. 2245-2254, doi: 10.1109/TPDS.2013.181

[12] Keromytis A, Misra V, Rubenstein D, SOS: An architecture for mitigating DDoS attacks, IEEE Journal on Selected Areas in Communications, 2004, vol. 22, no. 1, pp. 176-188, doi: 10.1109/JSAC.2003.818807

[13] Mousavi S, St-Hilaire M, Early detection of DDoS attacks against SDN controllers, 2015 International Conference on Computing, Networking and Communications (ICNC), Garden Grove, CA, USA, 2015, pp. 77-81, doi: 10.1109/ICCNC.2015.7069319

[14] Saied A, Richard O, Tomasz R, Detection of known and unknown DDoS attacks using artificial neural networks, Neuro computing, 2016, Volume 172, Pages 385-393, ISSN 0925-2312, https://doi.org/10.1016/j.neucom.2015.04.101-393

Sirisha Potluri, S. Sunaina, P. Neha, Ch. Govind, J. Raghavender, V. MNSSVKR Gupta

A Secure Cloud Infrastructure towards Smart Healthcare: IoT Based Health Monitoring

Abstract: The magnitude of big data is estimated to grow in the field of healthcare. Big Data when focused on the sector of health care can be best described as structured, unstructured and semi structured way of representing a patient's personal data such as his/her medical conditions, prescriptions, etc. Handling and processing such huge chunks of data can be a daunting task. To avoid scenarios of this type, many of the healthcare sectors have adapted cloud computing as the solution. Amidst the pandemic such as the novel covid-19, remote working has become the new normal. Healthcare sectors are gradually adapting to the idea of remote treatment also known as telemedicine. A patient's medical condition has to be coordinated with a team of specialists, nutritionists, nurses, etc. By using cloud computing one can completely avoid a physical interaction, it's very useful in current situations like covid-19. Hence cloud computing is chosen by many health sectors to receive and store huge chunks of patients data and manage their electronic records. This huge chunk of electronic records helps in the process of mining the data, identifying the patterns and developments in the big data healthcare sector. Main things that are to be taken care of : Privacy related issues and Security related concerns, Dynamically acceptable storage, Regulatory issues , Electronic documents containing patients data, handwritten medical editions ,various images such as X-ray, MRI scan, radiology images, etc. can be retrieved at any time and from any place. This

Sirisha Potluri, Department of CSE, IcfaiTech (Faculty of Science and Technology), ICFAI Foundation for Higher Education, Donthanapally, Shankarpalli Road, Hyderabad, Telangana 501203, India, sirisha.vegunta@gmail.com
Sai Lalitha Sunaina, Department of CSE, IcfaiTech (Faculty of Science and Technology), ICFAI Foundation for Higher Education, Donthanapally, Shankarapalli Road, Hyderabad, Telangana 501203, India, sunaina7571@gmail.com
Neha Pavuluri, Department of CSE, IcfaiTech (Faculty of Science and Technology), ICFAI Foundation for Higher Education, Donthanapally, Shankarapalli Road, Hyderabad, Telangana 501203, India, nehapavuluri99@gmail.com
Chennu Sai Sri Govind, Department of CSE, IcfaiTech (Faculty of Science and Technology), ICFAI Foundation for Higher Education, Donthanapally, Shankarapalli Road, Hyderabad, Telangana 501203, India, govindchennu@gmail.com
Raghavender Rao Jakileti, Department of CSE, IcfaiTech (Faculty of Science and Technology), ICFAI Foundation for Higher Education, Donthanapally, Shankarapalli Road, Hyderabad, Telangana 501203, India, jakiletiraghu@gmail.com
V. MNSSVKR Gupta, Department of Computer Science Engineering, SRKR Engineering College, Chinnamiram, Bhimavaram, Andhra Pradesh 53420, India, guptavkrao@gmail.com

https://doi.org/10.1515/9783110732573-004

can be an advantage and a disadvantage at the same time. The main challenges involved are failures of the network, security related concerns, and privacy related issues of patient information that is being ill-treated by users/customers, hackers, network downtime, malware, and etc.

Keywords: Cloud Computing, Virtualization, Data Security, Cryptography, Denial of Service, Health Care, Big Data, Blockchain

1 Introduction

Cloud computing is a distributed computing model, helps in delivery of computer system services including computing power and data storage. Cloud model uses dynamically provisioning of resources to meet the varying and dynamic resource requirements of a customer by the concept of distributed systems in which various virtual machines are grouped together. Virtualization is the core and has an important role in cloud computing. Virtualization technology involves creation of a virtual version of a server, a storage device, a desktop, an operating system. Programming level virtualization helps in PaaS offerings whereas IaaS is based on the idea of hardware virtualization [1].

In the last decade, information technology has played a major role in the field of healthcare. Many of the healthcare sectors have adapted cloud computing as the solution. Hospitals and healthcare providers are exempted from the need to purchase the hardware and servers. You can have huge cost savings by only purchasing the resources you actually use with the help of cloud. Patients can have control over their own health by using Cloud computing which democratizes data. By storing Patient records and medical images on the cloud, data can be easily retrieved. With help of Cloud computing healthcare providers can give prescriptions and treatment protocols by easily gaining access to the patient data. Irrespective of geographical locations Cloud computing also helps the specialists to review patient cases and give their opinions. A number of healthcare-related utilities such as telemedicine, pre- hospitalization, post-hospitalization etc. can be improved by applying cloud computing models in healthcare [2].

The primary concern in the healthcare practices and observations for online access of the EHR record -Electronic Health Record is Security and privacy. In order to protect the patient's information the sensitive records of Healthcare data should not be made available to unauthorized people. However cyber gaps in cloud computing posture an adversarial impact and influence on the security and privacy of patients' electronic health records. The online access of patient records and transactions related to diagnosis have many benefits for patients as well as healthcare organizations and professionals but it also raises serious security and privacy issues related to private data of patients. Due to risk associated with EHR record -Electronic

Health Record it is important to guarantee the privacy of patients. Hacking incidents on EHR record -Electronic Health Record systems may lead to modifying the data of patients.

The advent of big data has caused multiple obstacles in various research fields. The term “big data” refers to the vast and huge volume of structured and unstructured data. It consists of patient’s data and helps them to select the prime possibility and also to support the medicinal treatment plan. However, they have made hard to manipulate and process the data as the healthcare data became much larger. Contrastingly, the processing of big data on distributed sources is done by MapReduce. One of the main reason for faults in healthcare domains is the incomplete and imperfect access to patient-related data and information and unsuccessful communication among the stakeholders involved in the process [3].

2 Cloud Deployment Models in Healthcare

Cloud deployment models are represented in fig. 1 as shown below.

2.1 Public cloud

This type of cloud model is available for anyone who wants to use or purchase them. It is based on a shared cost model or pay per use policy.

2.2 Private cloud

This model is mainly used by stand-alone organizations. Private clouds are best for organizations that require high-security and high management demands.

2.3 Community cloud

Community cloud is a shared model that is limited to only a set of organizations or employees. This type of deployment model of cloud computing is managed and hosted internally or by a third-party vendor.

2.4 Hybrid cloud

Hybrid cloud combines two or more models such as public cloud, private cloud or community cloud. Based on business requirements Hybrid cloud architecture allows

an enterprise to move data and applications between private and public environments.

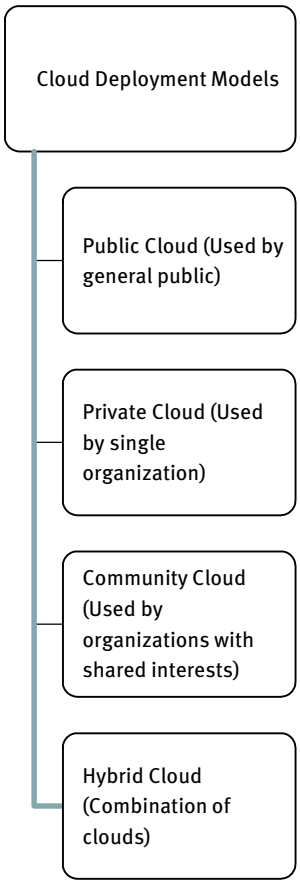

Fig. 1: Cloud deployment models for healthcare

3 Cloud Service Models in Healthcare

Cloud service models are represented in fig. 2.

3.1 Software as a service (SaaS)

SaaS describes a cloud service where consumers are able to access software applications running on a cloud infrastructure, over the internet. SaaS solutions do not

require the client to maintain anything, including the storage of data and the network and are managed by the vendor.

3.2 Platform as a service (PaaS)

Platform as a Service (PaaS) is an integrated and abstracted cloud-based model that supports the development, and management of applications. The whole storage and management of data is left to the vendor.

3.3 Infrastructure as a service (IaaS)

IaaS is the virtual delivery of computing resources in the form of hardware, networking, and storage facilities. Based on the amount of storage and the amount of processing power you use over a time period you will be charged according to that.

4 Factors to be Considered for the Evaluation of the Cloud System Security

4.1 Confidentiality

Confidentiality refers to protection of data from unauthorized users. In a Cloud System such users might want to get unauthorized access to the data of some other individual. Patient's information should be kept confidential in healthcare settings. Patient's reputation, opportunities, and human dignity may be under threat with inappropriate disclosure of that information.

4.2 Integrity

Integrity guarantees that the security property of an asset has not been modified by some unauthorized third-party personnel. It maintains the accuracy, reliability and consistency of data throughout its entire 'life-cycle.' Integrity ensures an asset's accuracy and correctness with respect to its owner. In healthcare, the accuracy of a patient's personal details, health summary, clinical notes, test results etc. can be maintained by integrity.

4.3 Availability

One of the most important aspects of security that needs to be maintained is Availability. A service-level agreement is a bond between the customer and the service provider about services to deliver in terms of availability and response to demand. Earlier, the SLA were negotiated between the service consumer and a client. But today there are different levels of SLA like customer based SLA, Service based SLA, Multi-Level SLA.

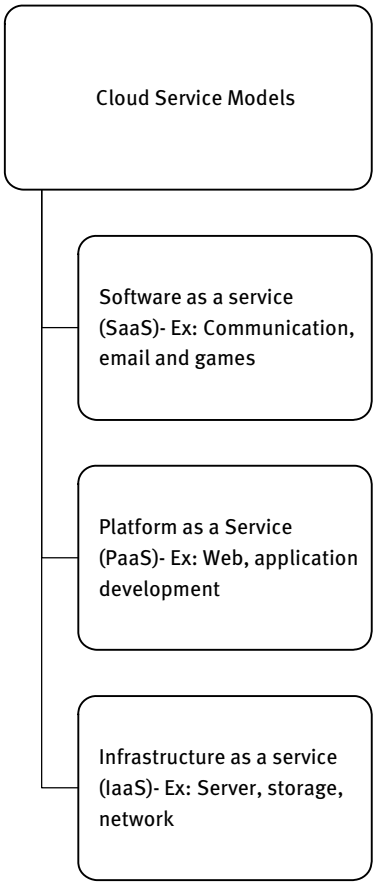

Fig. 2: Cloud service models for healthcare

Three important factors to be considered for the evaluation of the cloud system security are represented in fig. 3.

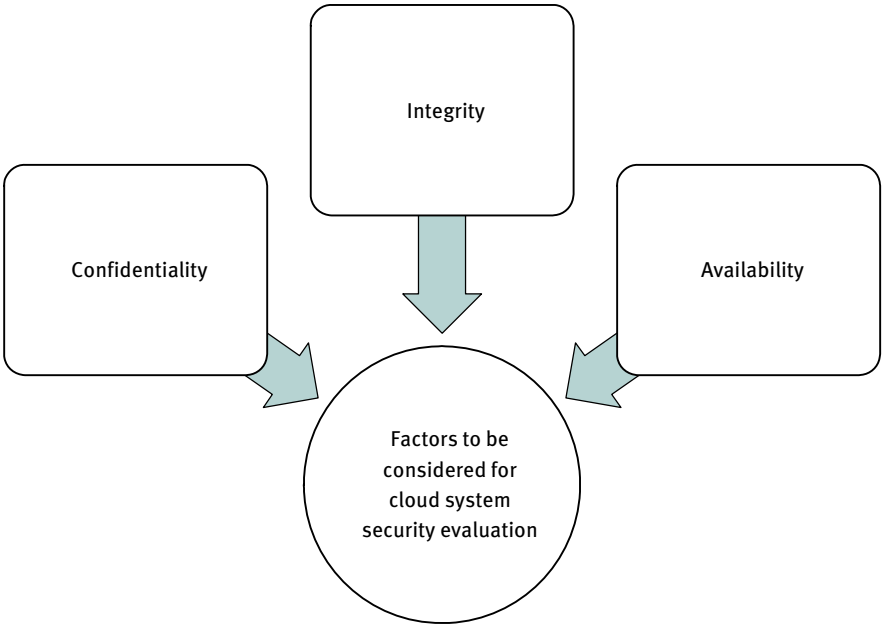

Fig. 3: Factors to be considered for the evaluation of the cloud system security

5 Review of Literature

Various security and privacy preservation methods and approaches in health care are discussed in table 1 as shown below.

Tab. 1: Security and privacy preservation approaches in cloud computing environment

S.No	Author	Title	Proposed Model
1	Jan de Muijnck-Hughes (2011)	Predicate Based Encryption focuses on both the Platform as a service and the Software as a service implementation	Predicate Based Encryption(PBE)
2	Venkata Sravan et al. (2011)	Security Techniques for Protecting Data in Cloud	Understanding security risks and the required security strategies used in Cloud computing to mitigate them
3	Ali Asghari Karahroudy (2011)	Security Analysis and Framework of Cloud Computing	Partially Distributed File System with Parity (PDFSP)

S.No	Author	Title	Proposed Model
4	Nabil Giweli (2013)	Enhancing Data Privacy and Access Anonymity in Cloud Computing	Data Centric Security approach
5	Miao Zhou (2013)	Enhanced Privacy Cloud keyword search and Remote public integrity audit for private data	Innovative tree-based key management scheme
6	Sudhansu Ranjan Lenka et al. (2014)	Enhancing Data Security in Cloud Computing using RSA Encryption and MD5 Algorithm	The RSA algorithm is used for encrypted correspondence and file encryption and decryption while the digital signature of the MD5 algorithm is used.
7	Aastha Mishra (2014)	Security and privacy of user's data	Advanced Secret Sharing Key Management Scheme
8	Nesrine Kaaniche (2014)	Cloud Data Storage Security based on Cryptographic Mechanisms	ID-Based Cryptography (IBC) and CloudSec
9	Afnan Ullah Khan (2014)	Data Confidentiality and Risk Management in Cloud Computing	Access Control and Data Confidentiality(ACDC)
10	Sarojini et al. (2016)	Trusted and Reputed Services Using Enhanced Mutual Trusted and Reputed Access Control Algorithm in Cloud	Enhanced Mutual Trusted Access Control Algorithm (EMTACA)

6 Recommendations for Smart Healthcare Model

Healthcare has one way of communicating with a patient i.e. through the internet via mobile devices and Laptop Considering the factors such as economic situations, location and affordability mobile devices are in demand. Since our main focus is to provide a secured and reliable healthcare service to a patient with the support of cloud computing services and facilities, we take the help of Paas, SaaS and BDaaS meaning Platform as a service Software as a service Big Data as a service respectively.

Analytical mobile applications helps us to analyze and filter the collected data beforehand so this is an added advantage compared to the normal mobile applications. These are built and hosted using cloud computing technologies. Mobile applications are accessed through web servers that run on mobile browsers without the considerations of mobile specific operating system, capacity and memory.

Cloud computing technologies includes delivery of various types of facilities as shown in fig. 4.

- SaaS (Software as a service): The provider platform consists of a residing software and the consumer can access it using a web browser or an API. It is a pay as you go model. Salesforce and office 365 are the examples
- PaaS (Platform as a service): An application is developed by the consumer and is hosted on a virtual server since the consumer has some control over data and applications it pushes to develop, test and deploy applications very fast.
- IaaS (Infrastructure as a service): IaaS is the virtual provisioning of the computing resources such as hardware, networking, and storage facilities.
- BDaaS (Big Data as a service): It delivers statistical analysis tools by an outside provider which helps the organizations to gain insights from a large information set to gain an advantage.
- NaaS (Network as a service): Network as a service defines services and facilities for network transport connectivity. NaaS contains the optimization of resource usage and allocations in view of network and computing resources as a cohesive whole.
- HaaS (Healthcare as a service): Infrastructure related to healthcare is delivered as a service and it can bring significantly cost effective solution for the healthcare organizations.
- MaaS (Manufacturing as a service): To ensure powerful transformation to automate various operations as various levels of manufacturing industries, MaaS is greatly used.
- IoTaaS (IoT as a service): Pioneering companies utilize information potential available through Internet of Things as a service to sense information and to create better products for customer satisfaction.
- AaaS (Analytics as a service): Analytics as a Service (AaaS) is a utility based service that offers a company with the proficiencies of a fully customized analytics platform for data analysis in cloud [4-9].

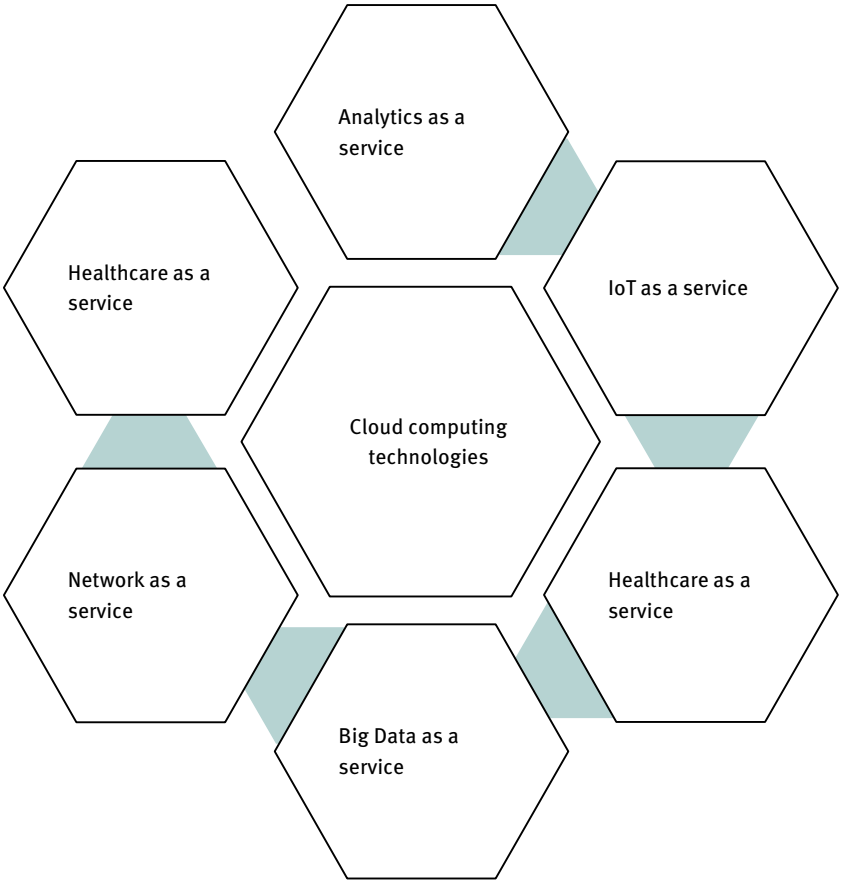

Fig. 4: Cloud computing technologies

7 Types of Cloud Architectures

7.1 Centralized

Clients are tied to the nearest data centres to avoid a high latency in communication because the cloud resources are partitioned over wide distances geographically.

7.2 Federated

Many small clouds together form a large cloud. It's very useful when the clients require a high confidentiality in data when distributing the data geographically.

7.3 P2P cloud

It's an extension of federated cloud architecture. The only difference is in p2p there are no centralizing and monitoring components. It consists of independent resources and peers and division of peer's costs is very low and it leads to minimal management.

Also in 2010, Koufi et al., have presented a model designed for pervasive access to cloud Emergency Medical Systems in short form namely EMS [10]. They present us with a new model of emergency medical systems in a cost effective manner. The key components of their system is as follows:

- Flexibility to meet ongoing demands
- Scalability to adopt dynamic changes
- Interoperability to understand and support system behaviour
- Execution and implementation of platform independent applications and policies: which ensure easy access and admission to the required data from anywhere in a distributed environment via any device

The important factors to consider from them are listed above and we want to take all these into consideration so we propose a model which has a p2p cloud architecture followed by a combination with BDaas, Saas and Paas. This is complying with all of the key components in their proposed system. There is scalability since in p2p there is no centralization and only consists of independent resources and peers. There is flexibility and interoperability in the services we provide and execution is the most effective trait of the proposed model. The model emphasizes on the combination of mobile applications and cloud computing.

Considering all the factors and different approaches provided by various authors and keeping in mind all the challenges are the failures observed in network, security challenges, and privacy issues of patient information that is being abused by users, hackers, malware, and etc. Conferring to the analysis and study of the above articles, many investigators and researchers have focused on reducing patient response time, increasing safety protection, and speeding up the medical treatment for patients, we take the help of Paas (Platform as a service), Saas (Software as a service) and BDaas (Big Data as a service) alongside P2P and that is our approach.

8 P2P Architecture

P2P cloud computing combines existing usages and technologies in a more interesting way. There are many security issues regarding user information, credit card

information, etc. Two methods that can help with this are Data security and connection security. Each storage device in P2P cloud architecture should use data encryption at a higher level.

This technique of storing data can ensure the content level protection such that stored data cannot be reached by those who have no privilege in accessing it. In a classic approach, users are directly connected to the servers via a protocol like a web service.P2P ensures there is a secured connection.

We believe combining P2P architecture and cloud computing is the best solution for analytics and management of big data. On one hand, P2P networking helps in decentralization such that peers can control their data and share resources via clouds. It also provides storage resources, computing and networking required for big data analytics. Overall architecture of P2P is represented in fig. 5 as shown below.

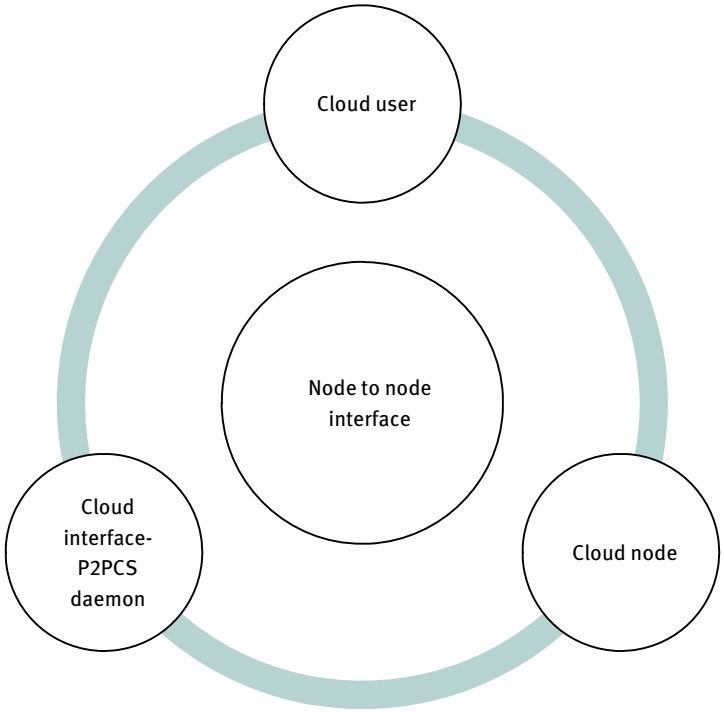

Fig. 5: Architecture of P2P for cloud platform

9 Security & Privacy

Data privacy makes sure that data is used appropriately and data is available to those who have authorized access. Privacy can be interpreted as an individual's right to determine to what extent information is communicated and how it is communicated to others.

The two main classes of data privacy are:

- Data is shared or released with third parties. This includes data collection, privacy-preserving and data integration data sharing and publishing.
- Privacy-preserving data mining.

A great deal of study has been carried out on the subject of privacy security, and in recent years there have been many significant review articles reviewing data privacy taxonomy, privacy protection mechanisms, proposed architectures, and data privacy protection methods; their advantages and disadvantages have been published. Suggested data privacy security techniques can be categorized into initial approaches, mathematical analysis, soft computing based on information and machine learning methods.

Privacy issue is one of the major threats in addition to loss of data, malicious modification, server crash are some examples of cyber threats such as Yahoo's three billion accounts exposure by hackers in 2013.

We proposed CNN based data privacy protection approach to ensure better quality standards in cloud computing environment. The extraction and inference phases of the function are divided here and the former takes place locally, while the latter takes place in the cloud. In this way, during the function extraction stage on the edge node, confidential information is extracted from the data and data transmission rates to the cloud are reduced. The privacy-preserving issue in the processing of data classification is taken into account through the application of deep neural networks. The CNN (Convolutional Neural Network) algorithm is used here as a deep neural network. Here, both in the learning and classification processes, a law-degree non-linear polynomial is replaced to obtain the high precision activation function. A classical deep neural network (with the ReLU activation function) is retained to provide data privacy security for the training process, after which the network changes only when it is used for classification. Combining the above polynomial approximation with batch normalization is the theoretical main innovation of this work.

In order to effectively solve the data privacy protection problem, encrypted storage of cloud data is a very outstanding solution. After encryption, the data is stored in the server provided by the cloud service provider in the form of cipher text, and in the meantime, the server is also required to return the data to the user when the user requires it. When the user needs to use the data frequently, it requires a lot

of network bandwidth and user's time to conduct communication with the server and realize data encryption and decryption, which will significantly reduce the usability of cloud computing. In the meantime, after the encrypted data stored in cloud servers has developed to a certain scale, effective retrieval of encrypted data has become a new problem that needs to be solved, while the traditional information retrieval technology can no long satisfy the requirement of mass data retrieval in the cloud storage environment [11-13].

10 Privacy Requirements and Issues in Healthcare as a Service

The following privacy requirements must be met to guarantee hospital and patient privacy.

10.1 Privacy of the hospitals' datasets

Each hospital documents the medical history and diagnoses of patients in its databases, forming a dataset that could be used as a PPRF algorithm training corpus. However, hospitals usually refrain from sharing them due to the sensitive existence of such information. Therefore, as we develop our model, their privacy must be ensured and protected.

10.2 Privacy of the hospitals' votes

Hospitals may choose to exclude a single or a collection of trees from the ensemble; however, information from their datasets may be revealed by exposing their votes. Hence, the votes of hospitals must remain private.

10.3 Privacy of the patients' diagnosed symptoms

A doctor will use the CDSS to retrieve potential diagnosis based on the patient's symptoms in order to diagnose a patient. If no assurances of privacy were provided, however, no patient would allow his or her symptoms to be fed into the system. The symptoms of patients must, therefore, remain private.

11 Cloud Services to Preserve Data Security in Healthcare

Preserving Data security is needed for the hour especially when cloud storage is used by various organizations of different fields ranging from educational institutions and huge MNCs relying on services like google drive to individual users like Dropbox, Box, Amazon Drive, Microsoft OneDrive etc. Such users trust these services and want to maintain their data's privacy by not letting it get corrupted or not losing it by any means. And if this trust continues millions of other users might want to store data on the cloud. Stored cloud data needs to be decrypted before a 3rd party could breach information since it is stored in an encrypted form. Adding to this. These are various methods by which users can inculcate their own security measures in addition to what is provided by the system. All things considered, there are still holes among practices and proposed arrangements, irreconcilable circumstances, and difference on prerequisites and ideas.

Comparison of cloud security and privacy preserving algorithms which are used in healthcare is represented in table 2 [14-21].

Tab. 2: Comparison of cloud security and privacy preserving algorithms which are used in healthcare

S.No	Model/Algorithm	Parameters
1	Bilinear pairing cryptography	Cost, time
2	Identity Based Encryption	Membership, identity
3	Homomorphic Encryption	Patient's data like clinical records, scanning and x-ray images
4	Attribute Based Encryption (ABE)	Security parameter, user data
5	Multi-Objective Privacy-Aware workflow scheduling algorithm(MOPA)	Storage cost, time, data,

12 Real Time Healthcare Dashboard- A Case Study Based on Blood Pressure Readings

Real time healthcare dashboard for tracking a patient health condition such as blood pressure readings, heat beat monitoring, blood sugar observing, cancer cell growth perceiving etc. is essential. Based on which we can perform time series analysis and go for a better prediction. The following code shows real time health care dashboard to monitor a patient.

Listing 1: Real time healthcare dashboard for tracking a patient health condition- blood pressure readings

```
# Real time healthcare dashboard for tracking a patient health condition
based on blood pressure readings
def _health_monitoring():
    arr_results = []
    client_record = WithingsApi(creds)
    health_readings = {
        # analyse readings based on past history
        'past_reading': {
            'x_p': '',
            'diastolic_p': '',
            'systolic_p': '',
            'pulse_p': '',
            's_m_average_p' : {
                'diastolic_p': '',
                'pulse_p': '',
                'systolic_p': '',
            }
        }
    }
 # Get patient readings
    p_measures = client_record.get_measures()
 # Get patient last reading date
    l_r_date = p_measures[-1].date
    p_counter = 1
 # Get patient raw readings from the record
    raw_readings_p = {
        'systolic_p': [],
        'diastolic_p': [],
        'pulse_p': [],
    }
# Extract patient measure
    for p_measure in p_measures:
        if p_measure.systolic_p_blood_pressure\
           and p_measure.diastolic_p_blood_pressure:
            next_pdate = l_r_date + timedelta(days=counter)
            # sort the values of date times
            health_readings['past_reading']['x'] += '"' +
p_measure.date.strftime('%Y/%m/%d %H.%M.%S') + '",'
```

```
            health_readings['future_reading']['x'] += '"' +
next_pdate.strftime('%Y/%m/%d %H.%M.%S') + '",'
            health_readings['past_reading']['systolic_p'] +=
str(p_measure.systolic_p_blood_pressure) + ','
            health_readings['past_reading']['diastolic_p'] +=
str(p_measure.diastolic_p_blood_pressure) + ','

raw_readings_p['systolic_p'].append(p_measure.systolic_p_blood_pressure)

raw_readings_p['diastolic_p'].append(p_measure.diastolic_p_blood_pressur
e)
            if p_measure.heart_pulse and p_measure.heart_pulse>33:
                raw_readings_p['pulse_p'].append(p_measure.heart_pulse)
                health_readings['past_reading']['pulse_p'] +=
str(p_measure.heart_pulse) + ','
            p_counter += 1
    return health_readings
```

13 Conclusion

Based on the investigations observed in the literature, the performance and enactment of telemedicine service through hosting and presenting options and choices of Amazon EC2. The efficiency and proficiency is examined and studied by answering the number of requests per seconds. According to the description provided by them, dynamic resource provisioning on web tier with medium type instances is much better than static allocation with large and extra-large instances. A feasible solution is obtained but it's not implemented in real time.

Cloud-based homecare cloud model is best suited for patients with respiratory diseases. They have a conscious platform that can dispense and store a patient's respiratory data alongside caregivers, families, and infirmaries quickly. By utilizing mobile technologies and models, the saturation and capacity of oxygen can be monitored and examined and the information can be distributed to patients and medical specialists.

In P2P there are no centralizing and monitoring components. It consists of independent resources and peers and division of peer's costs is very low and it leads to minimal management. The PaaS provider will fund much of the infrastructure and other IT related services, which users can access anywhere in a distributed environment via a web browser it is affordable as well PaaS offerings are usually used for mobile apps , cross platform apps and devops tools. SaaS and BDaas will help in the all-round development of cloud computing in healthcare.

14 References

[1] Rajkumar B, Chee Y, Srikumar V, James B, Ivona B, Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility, Future Generation Computer Systems, 2009, Volume 25, Issue 6, Pages 599-616, ISSN 0167-739X, https://doi.org/10.1016/j.future.2008.12.001

[2] Peter M, Timothy G, The NIST definition of cloud computing, National Institute of Standards and Technology: Special Publication (NIST SP), 800-145, 2011

[3] Al-Issa Y, Ashraf O, Tamrawi A, eHealth cloud security challenges: a survey, Journal of Healthcare Engineering, 2019, vol. 2019, Article ID 7516035, 15 pages, https://doi.org/10.1155/2019/7516035

[4] Harika K, Manisha G, Potluri S, An IoT based solution for health monitoring using a body-worn sensor enabled device, Journal of Advanced Research in Dynamical and Control Systems (JARDCS), 2018, Volume 10, Issue 9, PP: 646-651, ISSN 1943-023X

[5] Potluri S, Avinash M, Health record data analysis using wireless wearable technology device, Journal of Advanced Research in Dynamical and Control Systems (JARDCS), 2018, Volume 10, Issue 9, PP: 696-701, ISSN 1943-023X

[6] Avinash M, Potluri S, A study on technologies in cloud-based design and manufacturing, International Journal of Mechanical and Production Engineering Research and Development (IJMPERD), 2018, Volume 8, Issue 6, PP: 187-192, ISSN(P): 2249-6890, ISSN(E): 2249-8001

[7] Potluri S, Achyuth S, Elham T, Mohanty S N, IOT enabled cloud based healthcare system using fog computing: a case study, Journal of Critical Reviews, 2020, ISSN- 2394-5125, Vol 7, Issue 6, PP: 1068-1072, doi: 10.31838/jcr.07.06.186

[8] Goyal S, Public vs private vs hybrid vs community - cloud computing: a critical review, International Journal of Computer Network and Information Security, 2014, 6, 20-29

[9] Jansen W, Grance T, Guidelines on security and privacy in public cloud computing, NIST Special Publication, 2011, 800-144, pp. 5

[10] Koufi V, Malamateniou F, Vassilacopoulos G, Ubiquitous access to cloud emergency medical services, Proceedings of the 10th IEEE International Conference on Information Technology and Applications in Biomedicine, Corfu, Greece, 2010, pp. 1-4, doi: 10.1109/ITAB.2010.5687702

[11] Haider W, Iqbal W, Bokhari S, Bukhari F, On providing response time guarantees to a cloud-hosted telemedicine web service, Zhang Y, Peng L, Youn CH, Cloud Computing, CloudComp 2015, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 2015, vol 167, Springer, Cham, https://doi.org/10.1007/978-3-319-38904-2_24

[12] Risso A, Neyem A, Benedetto J, Carrillo M, Farías A, Gajardo M, Loyola O, A cloud-based mobile system to improve respiratory therapy services at home, J Biomed Inform, 2016, 63, 45-53, doi: 10.1016/j.jbi.2016.07.006

[13] Navimipour J, Navin H, Rahmani M, Hosseinzadeh M, Behavioral modeling and automated verification of a cloud-based framework to share the knowledge and skills of human resources, Computers in Industry, 2015, 68, 65–77

[14] Neghabi A, Navimipour J, Hosseinzadeh M, Rezaee A, Load balancing mechanisms in the software defined networks: a systematic and comprehensive review of the literature, IEEE Access, 2018, 6, 14159–14178

[15] Akinsanya, Opeoluwa O, Papadaki M, Sun L, Current cybersecurity maturity models: how effective in healthcare cloud?, CERC (2019)

[16] Duncan B, Pym D, Whittington M, Developing a conceptual framework for cloud security assurance, IEEE 5th International Conference on Cloud Computing Technology and Science, Bristol, UK, 2013, pp. 120-125, doi: 10.1109/CloudCom.2013.144
[17] Kumari S, Kamal A R, Optimal integrity policy for encrypted data in secure storage using cloud computing, Indian J Sci Technol, 2016, vol.9, no.8, 2016, pp.1–10, 2016
[18] Monikandan S, Arockiam L, A security service algorithm to ensure the confidentiality of data in cloud storage, Int J Eng Res Technol, 2014, 3(12), 1053–1058
[19] Shabbir A, Shabbir M, Rizwan M, Ahmad F, Ensuring the confidentiality of nuclear information at cloud using modular encryption standard, Security and Communication Networks, 2019, vol. 2019, Article ID 2509898, 16 pages, https://doi.org/10.1155/2019/2509898
[20] Singh N, Singh A, Data privacy protection mechanisms in cloud, Data Sci. Eng, 2018, 3, 24–39, https://doi.org/10.1007/s41019-017-0046-0
[21] Delettre C, Boudaoud K, Riveill M, Cloud computing, security and data concealment, Proceedings, 16th IEEE Symposium on Computers and Communications, Kerkyra, Greece, 2011, 424 431, 10.1109/ISCC.2011.5983874 2-s2.0-80052768216

I. Indrani, SVB Revanth, S. Akhil Durga, Sirisha Potluri, Sachi Nandan Mohanty

Internet of Cloud: Secure and Privacy Preserving Cloud Model with IoT Enabled Service

Abstract: Security and safety are among the critical difficulties of Internet of Things (IoT). Updating inappropriate gadgets, the lack of productive and powerful security meetings, customer ignorance, and viewing a well-known powerful gadget are some of the problems IoT faces. In this work, we explore the basis of IoT frameworks and security efforts, and we see other safety and security matters, methods used to verify IoT-based components and structures, security arrangements in place, and the best protection models are important and suitable for the various layers of IoT-operated applications. In this work, we have proposed another embossed IoT model: standard and expanded with security and safety components and layers of physical evidence. The proposed cloud/edge IoT framework is developed and tested. The background below spoke to IoT centres created via Amazon Web Service (AWS) such as Virtual Machines. The centre layer (edge) has been developed as a resource unit for Raspberry Pi 4 with the help of Greengrass Edge Environment in AWS. We used cloud-enabled IoT weather in AWS to create the top layer (cloud). Security meetings and basic management meetings were among all these areas to ensure the security of customer data. We have verified security announcements to allow data to flow between layers of the proposed cloud-enabled model. Not only does the proposed framework model eliminate the perceived security vulnerabilities, but it can also be used alongside the best security measures to combat network security risks facing all the latter layers; cloud, edge, and IoT

Keywords: Internet of Things, Cloud Computing, Cloud Privacy, Cloud Security, Edge Computing

Indrani Inapakolla, Department of CSE, IcfaiTech (Faculty of Science and Technology), ICFAI Foundation for Higher Education, Donthanapally, Shankarapalli Road, Hyderabad, Telangana 501203, India, indhrani1999@gmail.com
SVB Revanth, Department of CSE, IcfaiTech (Faculty of Science and Technology), ICFAI Foundation for Higher Education, Donthanapally, Shankarapalli Road, Hyderabad, Telangana 501203, India, svbrevanth162000@gmail.com
Siliveru Akhil Durga, Department of CSE, IcfaiTech (Faculty of Science and Technology), ICFAI Foundation for Higher Education, Donthanapally, Shankarapalli Road, Hyderabad, Telangana 501203, India, s.akhildurga@gmail.com
Sirisha Potluri, Department of CSE, IcfaiTech (Faculty of Science and Technology), ICFAI Foundation for Higher Education, Donthanapally, Shankarpalli Road, Hyderabad, Telangana 501203, India, sirisha.vegunta@gmail.com
Sachi Nandan Mohanty, Department of Computer Engineering, College of Engineering Pune, Wellesley Rd, Shivajinagar, Pune, Maharashtra 411005, India, sachinandan09@gmail.com

https://doi.org/10.1515/9783110732573-005

1 Introduction

Internet of Things (IoT) points to the concept of articles related to gadgets of many kinds on the Internet or wireless Internet. The popularity of IoT or Internet of Things has grown rapidly, as these new devices are used for a variety of purposes, including literature, travel, education and business improvement. IoT introduced the concept of connectivity, which means that organizations and individuals can communicate from far and wide easily. Kevin Ashton coined the term 'IoT' in 1999 to promote the concept of Radio Frequency Identification (RFID), which combines sensors and actuators. Nevertheless, the first idea was introduced in the 1960's. At the time, the idea was inevitable to register or install the Internet. Ashton presented the IoT's idea of promoting good exercise with chains. Be that as it may, the versatility of IoT has helped to boost strong availability during 2010. The Chinese government gave greater demand to the IoT by introducing a five-year plan. Approximately 26.66 billion IoT device resides in the rotating earth. The big bang started in 2011 with the introduction of home appliances, wearable gadgets, and sharp energy meters. The rapid explosion of IoT has helped organizations and in various ways improved statistical and business research methods. In addition, IoT has improved the way people live by introducing computer management. However, uncontrolled explosions have exacerbated security and safety challenges [1].

The unrecognized use, not the emergence of passwords, and the absence of updates to gadgets have increased the risks of online security and the acceptance of malicious applications on sensitive IoT frameworks. Such improper training increases the likelihood of information leaks and accidents. The vast majority of security experts view the IoT as a vulnerable area for digital attacks due to weak security meetings and arrangements. Unless a few security items are designed to protect IoT gadgets from digital attacks, security rules are not properly documented. In line with these lines, end clients have not been able to use defensive tactics to destroy information attacks. The developers of the program have created a variety of malware to contaminate IoT gadgets from the night before 2008. They are organizing various forms of crime to steal sensitive information in order to arouse public representatives to share sensitive information. Similarly, workplaces and certain companies are constantly facing security breaches due to prominent attacks. If gadget manufacturers and security experts assess digital risks accurately, they can create a protective component to prevent or kill digital accidents [2].

IoT enabled gadgets used for automated applications and for various business purposes. Applications help these organizations achieve their rivals. However, due to the unnecessary selection of various savvy gadgets that share information and connectivity, access to security and information becomes a major concern for many organizations, as it interferes with workflow, exercise, and organizational management. It is important for professionals to overcome these dangerous concerns and

make comprehensive safety efforts and strategies to protect the resources of their business and ensure the continued integrity and integrity of management. For example, powerful IoT kitchen appliances associated with a local organization can be a source of entry for planners to gain business acceptance and in addition to relevant information or to control and disrupt the business process.

New developments are emerging, or changes are being made in existing ones. Consider the latest developments in the 5G organization, for example. 5G is required to take a basic role in IoT frameworks and applications. It is upright enough to be recognized and is interested in the safety and security risks you can imagine, with its high frequency and data transfer. However, the shorter frequency necessitates adjustment at the base, as a result of which the need for additional channels to cover the same region is covered by new different remote techniques [3].

In this work, we plan to provide a framework for IoT applications, benefits, and expected risks. In addition, building a structure that needs to be considered and further enhances the best practice by doing or researching existing programs or developing new ones. Based on the findings, we offer suggestions for avoiding such dangers and treating potential safety concerns. This work will direct management organizations to continue to implement strategies, instruct storage clients and objects, and IoT-related partners to create and implement appropriate security and protection measures.

We developed our model using Amazon Web Service (AWS) as a confirmation of ideas, which later referred to real sensory frameworks that mimic the overall IoT structure. By creating a draft, we can post and consider different security measures by creating real locations and benchmarks.

We have embraced account research philosophy to explore a set of experiences and the basis of IoT frameworks, their security and security issues, and comparative measures. We have expressed our opinion about the inclusive and expanded IoT model and its protection and security. We designed and tested the cloud/elevated IoT model with the optical device (sensors), the hub edge (Raspberry Pi), and cloud management (AWS). This provision was intended to test the model we have proposed in the sections accompanying this paper. Our work does not give cunning to different IoT applications (well-being, intelligent urban communities, good chain, transport, etc.); their highlights, their preferences, and their challenges, or security risks that can be considered within these applications. The text is rich in such a thing. In this work, we wanted to have a complete review of the evidence and to lay the groundwork for further testing and evaluation.

The rest of the paper is organized as follows: the next section introduces bookkeeping followed by IoT security and protection challenges. In Section 4, we examine the end of the Internet of Things at the end. Section 5 introduces the proposed cloud-based/edge IoT models: standard and extended with protective and security components and layers of visual evidence. This section similarly illustrates the use of the proposed AWS cloud model and the conditions on the edges and package of the Raspberry Pi 4. Section 6 closes this function.

2 Review of Literature

The creators have pointed out that there are various problems, for example, sticking to and emphasizing attacks and other unauthorized access, which has reduced respect for customer information. There are potential programs that can assist a person in making various security measures that can help ensure their IoT gadgets. As mentioned, various security risks have arisen at the moment, and they can access IoT Technologies with their integrated organization. Organizations should provide testing and filtering tools to all IoT gadgets that can detect any type of risk identified safely and try to eliminate the risk of intrusion. Trainers and traffic analysts help identify and evaluate various digital risks [4].

Many administrators have introduced part of the difficulty or loading of widgets to various IoT gadgets and its porters. The different reproductive tools, models, and accessibility of the various components that can ensure this security meeting can also help to create a well-defined IoT security meeting for the novel. Most would agree with the rapid development of the IoT security tests and the various simulation tools as long as the actors supported this experiment. If IoT gadgets are likely to attack, then the problems will get worse.

The creators acknowledge that, while there are great benefits to clients for the Internet of Things, there are joining forces that should be taken seriously. Online security and security opportunities are the most important issues discussed. These two represent the tremendous difficulties in some business organizations as an open organization. The usual attacks of network protection have shown the weakness of new IoT devices. This is simply because the interaction of organizations on the Internet of Things brings openness to the anonymous and unreliable Internet, which requires security arrangements for novels. Also, it is important to emphasize the important norms and standards of the IoT Cyber Security framework regarding the creation of an IoT security framework. As noted, one of the key steps to consider is the conclusion of an agreement with a variety of gadgets with different book conferences. Differences in meetings prevent separate service contracts from operating and are essential elements to be found in the security structure of each Internet of Things network. He pointed out that to ensure the reliability of the IoT system in the online security sector, little progress should be made to help reduce the security complexity of the IoT network. Likewise, the founders have shown that doing more things is an important part of the success of the Internet of Things network security program. The researchers said the IoT climate should work with a variety of factors to address the billions of Internet-related challenges and network security. Accordingly, the journal has suggested that the weather protection of the IoT network should also keep testing, for example, installation testing, partial testing, framework testing, and consistency testing, adequately minimizing complications and

risks. In a similar vein, the creators have introduced part of the current IoT network security systems [5].

Some important safety efforts have been made by the provider, and have shown that it does not prepare the provider to make better arrangements. Due to the online protection of the Internet of Things, organizations will probably not make the necessary arrangements. Also, the creators are introducing real-time flexible and digital frames as a whole, from mechanical control frameworks, current vehicles to the basic framework. Recent features and functions, for example, Industry 4.0 and Internet of Things (IoT), ensure the innovation and innovation plans of new customers through a strong network and the effective use of the new age of installed gadgets.

These frameworks produce, rotate and trade a wide range of functional information. Security and the secretive beliefs that make digital attacks an attractive goal of the Internet of Things cause real corruption and disrupt people's lives. Network security and security are important on the grounds that they may pose a risk. The multiplicity of these frameworks and the potential consequence of digital attacks present new dangers in today's related IoT frameworks. Potential answers to the security and safety challenges are the standard security frameworks of modern IoT frameworks. The current IoT frameworks have not been adequately developed to ensure appropriate capabilities.

As such, there has been a remarkable increase in the investigation and evaluation of various security issues on the IoT. One of the main objectives of IoT security is to protect, maintain, and ensure that each client can develop the assurance, foundations, and assurance of access to the different management provided by the IoT biological system. Similarly, alternative IoT security testing enhances basic capabilities with the help of various recreational tools such as multi-component computers [6].

3 IoT Security and Privacy Issues

IoT has brought clients great benefits; however, a few difficulties joined in. Network security and privacy prospects are important concerns for analysts and security professionals in question. These two represent the great difficulties of certain business organizations such as open organizations. Outstanding network attacks have highlighted the weaknesses of IoT development. This weakness lies in the fact that organization's connections to the Internet of Things bring access to an anonymous and unreliable Internet that requires security arrangements for novels.

In the vast majority of known problems, none of them affect IoT variations, for example, security and protection. However, it is unfortunate that clients do not have the necessary assurance of security impacts until after the break has occurred, causing serious damage, for example, loss of important information. With the advent of

advanced security that has undermined customer protection, consumer's craving for helpless security is now diminishing. In an ongoing study aimed at security and safety, the Internet of Things customer service did not go well. There has been a ton of weakness in the current auto industry [7-8].

3.1 Safety

IoT is integrated from standard PCs and gadget registrations, making it incapable of dealing with security challenges of various types:

- Many Internet of Things gadgets are designed for large size layouts.
- Typically, IoT configurations contain a number of similar or almost indistinguishable resources with comparable features. This similarity enhances the magnitude of any security vulnerabilities that could completely affect a large number of them.
- This advancement means that the potential number of connections between IoT gadgets is staggering. It is even more certain that most of these gadgets can set up organizations and talk about different gadgets as a result in an unexpected way. This needs to be considered with the available devices, methods, and techniques available for IoT security.

Indeed, while the issue of data security and innovation is not a new phenomenon, the use of IoT has brought about different measures to lean towards. Consumers need to rely on Internet technology and management is safe from mistakes, especially as these innovations continue to gain more time and are incorporated into our normal days of life. With partially enhanced IoT devices and management, this is one of the major routes used for digital attacks such as the importation of customer information by leaving information streams unsatisfactory.

The concept of IoT gadget connectivity means that if the gadget is poorly verified and connected to it has the potential to influence global security and flexibility around the world. This behaviour is achieved by testing a large IoT gadget function. Aside from the ability of certain gadgets to have the option to interact directly with different gadgets, it means that clients and developers of IoT are all committed to ensuring that they do not expose separate clients such as the Internet itself from potential damage. The standard approach required to build a robust and efficient response to a crisis is as seen now in IoT [9-10].

In terms of validation, for example, IoT faces a different weakness, which remains a major problem in security systems in many systems. The authentication used is limited by the way it protects against just one risk, for example, Denial of Service (DoS) or retaliation. Data security is one of the most critical regions in IoT authentication due to the increase in unsafe use due to their diverse IoT climate information. If possible, for example, we have taken a picture of Visa contacts.

These cards are equipped to allow card numbers and names to be used without IoT verification; this makes it possible for program planners to have the opportunity to purchase merchandise using the cardholder's financial balance number and their personality.

Another notable attack on IoT is the man in the middle, where an outdoor photography channel is shown to photographing characters of large areas involving network trading. The man, at the centre of the attack causes the bank employee to see the exchange as a legal term because the enemy does not need to know the character of the suspect.

3.2 Secret

The concept of easy-to-use IoT depends on how well it looks at people's safety preferences. Concerns about the safety and potential harm of joining an IoT may be crucial in maintaining full IoT acceptance. It is fundamental to see that customer protection and management rights are critical to ensuring customer confidence and confidence in the Internet of Things, compatible gadget, and related advertising management. A lot of work is trying to get the assurance that IoT is reconsidering security issues such as increased monitoring and tracking. The explanation behind the concern for security is the direct result of the inevitable understanding of the complexity of the past where the cycle of testing and dissemination of data on IoT can be done almost anywhere. Universal access to the Internet is equally a fundamental figure that helps to understand this problem on the grounds that unless there is an exciting system, then it will be explicitly acceptable to access individual data from any aspect of the earth [11].

3.3 Cooperation

A separate climate for IoT specialization is known to suppress customer motivation. Apart from the fact that full integration is rarely practical in real estate and management, clients are reluctant to purchase and manage items when there is no flexibility and concern about getting inside the vendor. Inadequate IoT naming can mean that there will be a negative reversal of the assets of the management systems we work with.

Cryptography is one of the most widely used cornerstones to provide security in many ways. A powerful system of self-defence against potential attacks is not considered using a single security system. This, in turn, requires different levels of protection from the risks of IoT authentication.

By improving the improved safety points and adding these excellent features, hacks can be prevented. This avoidance is due to the fact that clients will purchase

items that currently have legal security that exposes the preventing vulnerabilities. Online security programs are part of the measures in place to ensure IoT is secure.

Alternatively, features and minor concerns may affect the negotiation efforts of the Internet of Things gadgets; this includes:

- Periodic updates: for the most part, IoT manufacturers are updating security updates on a quarterly basis. OS forms and security patches are also redesigned. In this way, program planners get ample opportunity to break the security conventions and take the details involved.
- Embedded passwords: IoT gadgets store embedded passwords, enabling help professionals to investigate OS issues or deliver important updates remotely. Alternatively, programmers can use the feature to securely access gadgets.
- Automation: regular, performance and end customers using computer equipment for IoT social media frameworks or to improve business practices. Alternatively, if retaliatory areas are not displayed, the installed AI can access those resources, which will allow risks to enter the framework.
- Remote access: IoT gadgets use various organizational conferences for remote access such as Wi-Fi, ZigBee, and Z-Wave. Often, clear limitations are not addressed, which can be used to deter cybercriminals. Therefore, program planners can quickly establish a revenge organization through these remote access conferences.
- Several integration of external applications: a number of application programs are available online, which can be used by organizations to perform specific tasks. In any case, the functionality of these applications was not detected without a problem. In the event that final clients and representatives present or access such programs, risk specialists will enter the framework and damage the database.
- Incorrect gadget authentication: most IoT applications do not use authentication management to block or limit network risks. In this way, the attackers enter the entrance and undermine security.
- Weak Device Recognition: In general, all IoT manufacturers set up identifiable gadget identifiers to monitor and track gadgets. In any case, few manufacturers do not keep their safety strategies. After all, following questionable internet tests becomes very dangerous [12-16].

4 The Future of IoT

At the moment, objects and structures are enabled for network access and have the ability to register to talk about compatible gadgets and devices. Increasing the capacity of the organization in all areas of thought will make our lives more successful and help us set aside time and money. Besides, connecting to the Internet more and

more aims to talk about the dangers of digital. Web-authorized content becomes the responsibility of cyber criminals. The expansion of the IoT market increases the magnitude of the potential risks, which could affect the profitability and well-being of gadgets and therefore our security. Reports include the frequency of information breaks that are definitely extended since 2015; 60% in the USA only. A review of all that has led to Japan, Canada, the UK, Australia, the USA and France found that 63% of IoT consumers thought these gadgets were a threat due to poorly regulated security. The test findings also included that 90% of customers are unsure about IoT network security.

Momentum research has investigated various creative processes to measure digital attacks and enhanced security arrangements. Part of the experimental detected arrangements are recorded below; Transfer encryption processes: authorizing robust and robust encryption methods can extend online protection. Encryption assembly performed on both cloud and gadget environments. As a result, the editors of the program were unable to comprehend the intangible and abusive data structure. Consistent assessment of emerging risks: safety risks are regularly assessed. Such groups analyse the impact of IoT threats and develop effective control measures through continuous testing and evaluation.

Adding duplication of updates: gadget manufacturers should grow fewer fixes than counter important updates. Such a procedure can reduce the uncertainty of starting the adjustment. Also, continuous updates will help clients by misleading dangerous digital assets from various sources.

Transfer solid gadget test devices: a large part of the new test is designed to make heart-focused gadget viewing strategies so that those questionable tests can be tracked and controlled without any problem. Many IT organizations are familiar with a gadget capable of viewing hazardous materials. Such devices are very important in risk assessment, which helps organizations to build modern control tools.

Create archived customer rules to create security assumptions: a large part of the break breaks and IoT attacks occur due to a lack of customer thinking. For the most part, IoT security efforts and regulations are not identified when clients purchase these gadgets. In the event that gadget makers explicitly determine potential IoT risks, clients may end up with these issues. Organizations can similarly organize preparatory projects to improve security awareness. Such projects guide clients to build strong passwords to update them consistently. Also, clients are told to restart security adjustments consistently. Clients add more and are said to maintain a range of strategies from spam messages, external applications, or sources that can sell IoT security.

There will be more than 30 billion IoT gadgets by 2025. Before that, people knew about IoT work, yet they discarded the idea by looking at how confusing the idea looks and how tempting it is to do it. However, with the development of new inventions, it is now possible for people to believe that this is only possible as the level of development of IoT increases the new steps step by step. In 2020 and earlier, for

example, intelligent home controls and bright lighting are just a few examples of how IoT is used to protect energy and reduce tariffs and this can add to the amazing motivation of why so many people choose IoT gadgets.

Many urban communities will shine. There will be better traffic management; roads will be freed from closures, urban areas will benefit from reduced pollution, safety will be the high expectations for this with a massive IoT massacre.

Management of medical care is very expensive, with the majority of diseases persisting in ascendancy. We are heading for a time when essential medical services can be integrated to find other people, especially as people are more prone to infection. Other than that, apart from the fact that the new product is not designed to prevent people from growing, it could help make medical services easier on the pocket to the point of availability. For example, by delivering regular clinical checks from an emergency clinic to a patient's home, this will be of great help to patients. Ongoing testing using Internet-related gadgets is one of the ways in which it will help save the lives of many patients. Timely alarms are critical in case of emergency situations, the same number of IoT gadgets in clinics will continue to be associated with the most important details for continuous follow-up. Patient satisfaction will be fundamentally improved.

In this work, we propose another perspective on IoT models: inclusive and extended with security and security components and ID and team layers. We have designed a cloud/raised edge of the IoT framework to make the proposed IoT models. Therefore, in this work we begin by introducing inclusive and expanded models, at which point we demonstrate our experimental design and climate (use of a concentrated model), and then present and discuss the results and findings [17].

5 Generic IoT Layers and Data Integration Model

The standard design of the IoT model, from the creator's point of view, is uncertain as to whether there are any comparable observations in writing, as shown in fig. 1, containing gadget, cloud and end customer layers. The gadget layer consists of a pool of Internet-enabled sensors, data acquisition hardware, and book conferencing to send information to the nearest or remote capacity for additional preparation. These gadgets allow the client to collect data on an ongoing basis through various purchase waves. Cloud layer contains data collected from additional management sensors, audio output, including output, and data scripting. This information is later regarded as a network of emotional selections that conducts the investigation of complex data and man-made knowledge to provide an option in relation to human well-being. The final client layer, which consists of the receiving client, can be in various frameworks. Of concern are smart gadgets, where safety and security challenges exist. Within the boundaries of these three layers, a rundown of sublay-

ers or modules is installed to ensure the strength of the air support network. To ensure that data is sent and managed quickly to provide basic options that will not stand until the data is sent to the cloud, we present the edge-finding capabilities that can stay in such a great option, and simultaneously save duplicate information and send it to cloud layer to prepare and store long-term retrieval. In some cases, we need to send orders or references to certain wearable gadgets to update their purchase or usability ratio, and this will require alternative assembly and security measures.

Fig. 2, shows the extended extension of the excluded model. We are seeing an expansion of new layers; on the brink of misery. These two layers can overcome the issues of inactivity from the dependence of the benefits of the cloud layer and can be resolved in a quick selection. Edge registration occurs on gadgets where the sensors are plugged into or actually turned off. They provide continuous selection and control over the sources of information, and at the same time, discuss the various layers to convey information by integration, remote, and investigative. The haze enrolment layer motivates edge-testing experiments on all the most notable intellectual property associated with neighbours and is actually removed from the nerves and sources. These additional benefits create significant safety and security challenges [18].

6 Security and Privacy Policies

Cloud-based management is often regarded as the basic IoT framework that provides information storage, data preparation and information sharing. Program planners and abusers focus on IoT processing gadgets and on hubs that store or transmit sensitive information. For example, tolerable data and electronic clinical records make the medical services framework an important part of the program. Each layer of the IoT model presents security challenges and, at the same time, the opportunity to maintain safety and security practices and meetings. For example, in the gadget layer, sensor information is sent to the edge, in the haze, and then to the cloud, the requirement of approval and announcements that trust explicit workers to mitigate these attacks. Firmware and machine address security ensures and that is the only snow, however, this comes as a result of power consumption, as part of remote-enabled gadgets, for example, wearable battery-powered. Those safety efforts must be revived to achieve both safety, and power [19].

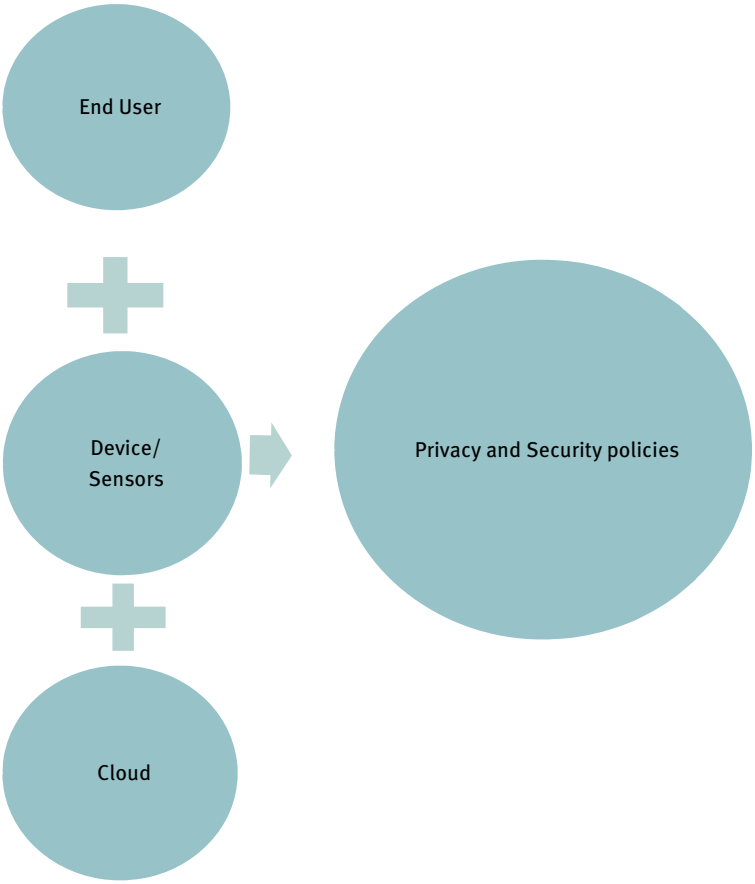

Fig. 1: Internet of Things (IoT) generic model with privacy and security policies

On the cloud layer, security efforts need to ensure organizational meeting between edge areas and mass areas and periodically from sensors. Converting meeting messages, highlighting encryption points, and enabling all provides minimal information for check-in and login. At the data management and final client level, we need to ensure that data retention and retrieval of fixed data is protected from SQL attacks, smells, and attacks of sensitive identity theft documents, providing renewable support and following HIPPA procedures (in social frameworks) [30)]. The integration of the information can familiarize the department with the programmers to isolate the client, as a result of which security comes in. As IoT gadgets can join and leave the organization of sensors and sources, this can add a lot of confusion to the general security effort strategies, hence the need for new smart and diverse security efforts [20].

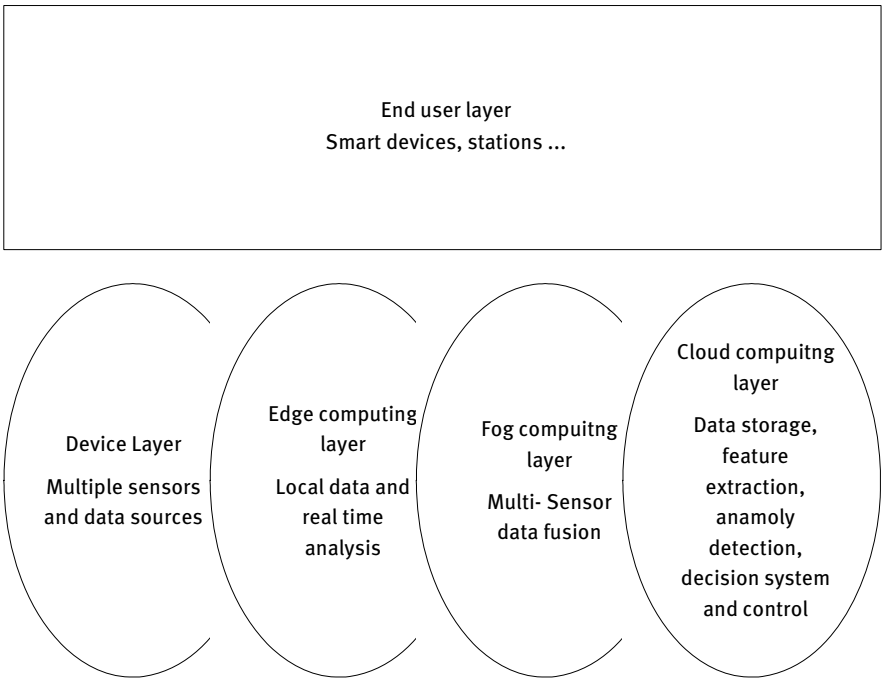

Fig. 2: Cloud Edge IOT model

7 Implementation of the Recommended Cloud-Edge-IoT Model

Our approach to ensuring security measures put in place before sending enabled gadgets to IoT has been proven in terms of planning and ensuring that they can safely transfer and share information, protecting data encryption. Fig. 3 below shows the emergence of machinery, system, and book model. The model contains AWS cloud as expert cloud, Raspberry Pi 4 as Edge Node, and Virtual Machines as IoT gadgets. The framework we have created is a paid AWS record for full acceptance of assets provided by AWS, including testament keys and encryption, approval and validation.

From the assets acquired by AWS, we have implemented AWS Identity and Access Management (IAM) web administration. It allows us to control client login by setting up an IAM (customer representation) account for all clients. For security reasons, we did not use the AWS Root account but started the IAM client with authorized authorization. Designing the Raspberry Pi as an Edge hub (AWS Green grass Core), AWS Green grass Core works directly with the cloud and works locally.

The Raspberry Pi was designed with an outstanding addition to the Linux durability. Creating a partnership between AWS and Raspberry. We used the AWS Green grass Core to create a circle with the centre gadget, as well as any remaining IoT gadgets to allow them to speak on the edge.

We need announcements to verify all gadgets with AWS. We have issued recommendations, private and public keys for safe and secure relations with AWS. Institutional certification is generated by AWS once we have done the Greengrass circle, as shown in Fig. 4 below. We downloaded the documents produced on the Raspberry Pi and started Green grass Core.

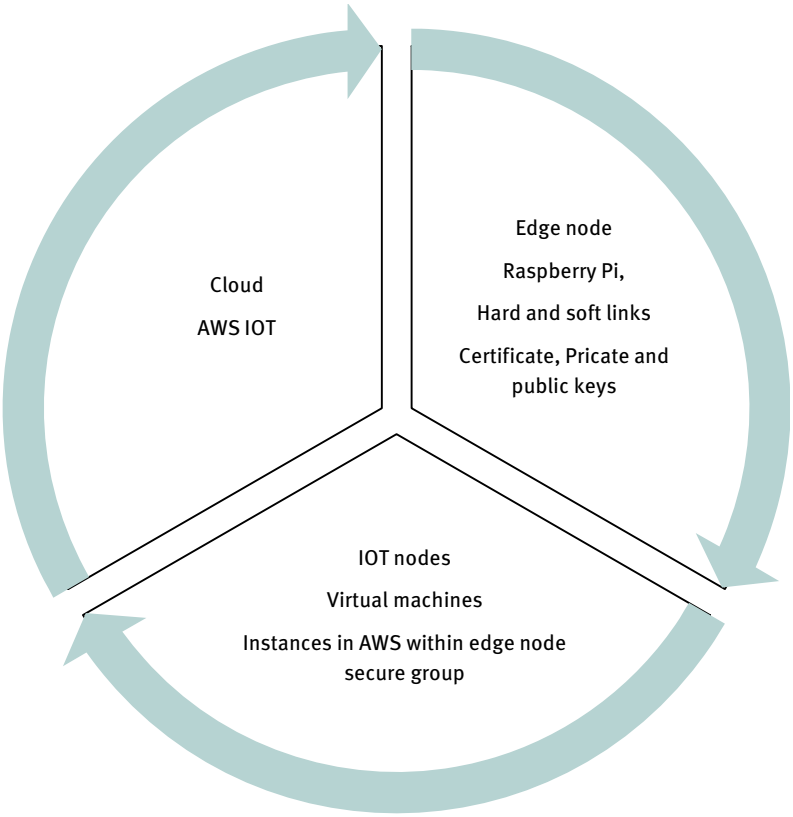

Fig. 3: The proposed model

8 Discussion and Analysis

IoT gadgets are classified as virtual machines, made into AWS, and added to the Greengrass facility, as shown in Figure 4 below. At the time of creation, a special announcement was made, public and private keys to all gadgets to verify them through AWS and the Greengrass Core gadget. The connection between the two gadgets is made through a secure system using an MQTT session called the message vendor. Finally, Fig. 5 shows both IoT and Edge hub facilities being successfully deployed and information trading completed at specific times.

The following are some key points to keep in mind about our AWS workspace and model used:

- In every model, IoT gadgets are either portable or come with AWS IoT Core.
- In our model we added an edge view using the Green grass IoT centre view on AWS, and spoke to it via Pi, so that we could see it as an additional middle ground between IoT and AWS IoT Core gadgets and then a cloud.
- Each gadget needs its own authentication, private key, and CA Root announcement (this is an AWS IoT agreement). There are different types of CA Root agreement based on IoT gadget types.
- Each gadget needs a strategy, this setting indicates which functions this gadget can perform (interface/find/distribute/purchase, etc.)

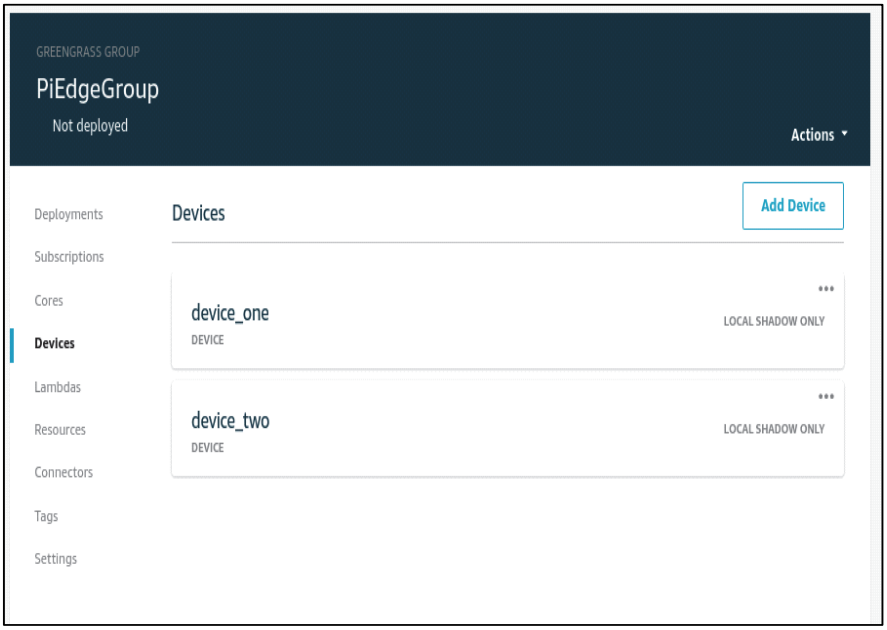

Fig. 4: IoT-enabled nodes

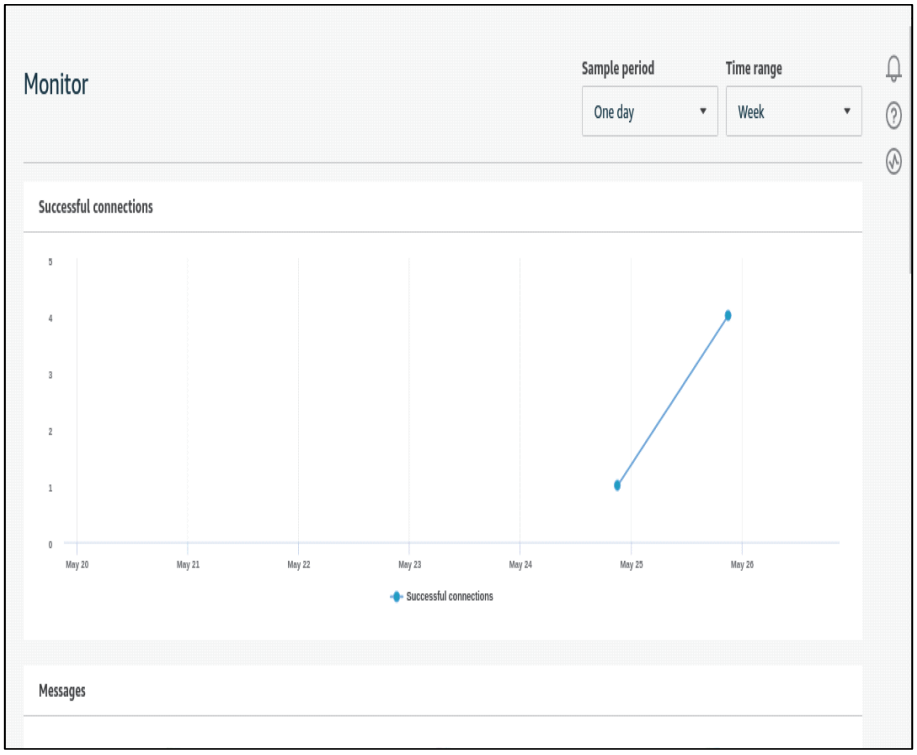

Fig. 5: Successful communication and data exchange between nodes

The x-axis: days of the month, and the y-axis: the number of connections. Along these lines, we made a gadget, strategy, and testament. At that point we joined the arrangement to the declaration, at that point appended the authentication to the gadget. A default strategy is demonstrated in the code listing beneath:

Listing 1: Default device policy in Amazon Web Service (AWS)

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
           "Effect": "Allow",
           "Action": "iot:*",
           "Resource": "*"
       }
    ]
}
```

8.1 Key points of proposed model

- Default strategy allows the gadget to play all functions (Action: iot: *) from any remaining gadgets (App: *).
- In our model, we have developed a modified strategy to deal with an additional layer of grass.
- Addition, activity: green grass: * means that the gadget in the green grass circle can play all functions from and to different gadgets in the same green grass circle (App: *).

The modified version of our model appears in the following code listing. In our case, the books are finalized using the MQTT assembly which is a machine assembly system. MQTT is used for reasons that it is lightweight (small-sized messages and requires low power), so it makes sense for forced weather (sensors as a metaphor for real applications).

Listing 2: Modified device policy to include the edge layer in the proposed model

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
           "Effect": "Allow",
           "Action": [
"iot: Publish",
"iot: Subscribe",
"iot: Connect",
"iot: Receive"
],
           "Resource": [
                "*"
            ]
       },
       {
           "Effect": "Allow",
           "Action": [
"greengrass:*"
           ],
          "Resource": [
                "*"
          ]
       }
    ]
}
```

In addition, note that IoT gadgets in AWS are copied as MQTT clients (if they are visible - in what is important in our case), and MQTT clients transmit the MQTT title. The association can be regarded as a secure channel between customers, it is formed, at which time customers can buy from it, and various customers spread the message to it.

Now, the Raspberry Pi setup process involves installing JAVA JDK8, green grass files, in addition to the appropriate Core software (depending on the device used — for us, it's Raspberry Pi 4).

All these files have been transferred to Raspberry Pi 4 as shown in Fig. 6 below.

Fig. 6: The Raspberry Pi 4 kit setup

After the exchange of fundamental documents to the Raspberry Pi 4, we expected to extricate them and roll out certain improvements on some arrangement records, to coordinate the created testaments and keys. At last, we began the Green grass centre gadget.

Fig. 7 underneath shows that our Raspberry gadget effectively filled in as an Edge.

Fig. 7: Running Greengrass successfully on the Raspberry Pi 4 kit

After setting the weather and making sure it was right, we made the MQTT theme for our situation and named it (my/point). At that time, we made the gadget to be purchased on my/subject and made another gadget to be the presenter on my/theme. All technologies can play all functions with any remaining gadgets (default strategy), and all messages are successfully sold. Fig. 8 shows the different types of messages traded in one day. Meeting time is influenced by many factors including the inertness of the organization and the pre-management stage.

The proposed IoT model has shown that we can ensure the safety and security measures put in place before allowing the IoT enabled gadget or hub to transmit or share its information. When properly designed and built, we ensure that our resources are secure. The model shown in this paper can be used to provide secure IoT shapes and structures with haze/edge processing layers and a combination of sensors. Some real-time applications can use this model, for example, medical care, military, debacle recovery, and many more. Allow us to look into the case of medical services; for example, through a proposed strategic-based model, clients will be able to trust their medical service providers to allow them to be protected to see that they are being cared for. Medical care organizations incorporate resources into clothing with the assurance that they will help improve employee benefits, reduce unemployment, and reduce the cost of medical services. Another major factor in wearable gadgets is the belief that it can provide for people with disabilities. For example, a person with special needs will have the option of placing orders and text, say, by moving a finger here and there. The final, but unrestricted, strategy is the number of security customers who can work on their records. For example, individuals can classify who can see their social media posts or policies that specify the amount of additional security is added to their record (e.g., two-factor authentication)

While the developers of IoT applications (medical services for this condition) try to do the best for their customers, there are still a few principles that will fail. One of the inefficiencies will be how client information is removed and how outsiders handle it. It is often up to the supplier himself to ensure that they set the rules and propose an arrangement that will enable them to behave responsibly with vendors and their customers. The same thing applies with customer segregation. More often than not, outsiders, (for example, insurance agencies) can obtain customer data in case they “agree” with it, and then from there, it can be dangerous to determine if it is solid. In the following figure, on the X- axis hours of the day and on the Y- axis one day message readings are represented.

Fig. 8: Successfully exchanged messages of different types: PublishOut.Success, PublishIn.Success, Connect.Success, Ping.Success, Subscribe.Success

9 Conclusion

IoT devices and applications play an important role in our modern life. We can see IoT devices almost everywhere from our homes, offices, shopping centres, schools, airports, and many other places to provide us with secure and sought-after services.

IoT gadgets support collaboration with partners and help in understanding business needs and outcomes. In addition, IoT-based testing and information processing can enhance the profitability and productivity of a modern framework

In addition, IoT frameworks are implementing a variety of innovative new development applications in a variety of areas. Retailers and many organizations are finding a large proportion of arrangements to protect their gadgets related to malicious attacks. With the large number of these gadgets associated with our private organizations and the Internet, additional concerns and protections are also being taken into account. We read and hear that our espresso machine is watching our conversations; our excellent department sends our guests photos of government agencies. Some real models emphasize the seriousness of the security vulnerabilities associated with the use of IoT gadgets.

In this work, we have introduced new IoT models: standard and accessible with insurance and security components and highlights. The proposed cloud/edge structure is maintained and tested. The low level is considered by IoT institutions developed by Amazon Web Service (AWS) as Real Machines. Medium level (Edge) has been achieved as a Raspberry Pi 4 gear pack with a source of Greengrass Edge Environment in AWS. The high level, which is a cloud, is eliminated using IoT cloud

computing in AWS. Security meetings and basic management meetings were held between each of these layers to ensure the protection of customer data

In the future work, further research should be done on cryptographic security strategies that are best suited to operating IoT-compressed IoT (Light Weight Crypto) devices. It will help to ensure that clients with a variety of connections can use and set up IoT frames without the lack of consumer integration that comes with the large number of these IoT gadgets. In addition, there is a real need to make a variety of information and sharing methods available for Internet-related IoT gadgets. Such guidelines will reduce the number of unexpected vulnerabilities and related attacks in non-identical categories.

We study the benefits and risks associated with IoT. With all the various benefits, risks can be misused to harm end clients by allowing unauthorized acceptance of sensitive information, enabling framework attacks, and endangering the health of individuals. With IoT enabled gadgets marketed, we need to deliver them with appropriate security efforts that facilitate their use, function, and join existing structures. We relied on the help of analysts to create a unique security structure to reduce, not really kill, security and protection opportunities, and be bright enough to adapt to changes in the new literature development and various organizational conditions for application.

10 References

[1] Sharma N, Shamkuwar M, Singh I, The history, present and future with IoT, Balas V, Solanki V, Kumar R, Khari M, Internet of Things and Big Data Analytics for Smart Generation, Intelligent Systems Reference Library, 2019, vol 154, Springer, Cham, https://doi.org/10.1007/978-3-030-04203-5_3

[2] Khanna A, Kaur S, Internet of things (IoT), applications and challenges: a comprehensive review, Wireless Pers Commun, 114, 2020, 1687–1762, https://doi.org/10.1007/s11277-020-07446-4

[3] Chang D, Chen Y, Chen L, Chao C, Internet of things and cloud computing for future internet, Chang S, Kim T, Peng L, Security-Enriched Urban Computing and Smart Grid, Communications in Computer and Information Science, 2011, vol 223, Springer, Berlin, Heidelberg, https://doi.org/10.1007/978-3-642-23948-9_1

[4] Heena W, Rajni A, Fog computing with the integration of internet of things: architecture, applications and future directions, 2018, 987-994, 10.1109/BDCloud.2018.00144

[5] Adel A, Utilizing technologies of fog computing in educational IoT systems: privacy, security, and agility perspective, J Big Data, 2020, 7, 99, https://doi.org/10.1186/s40537-020-00372-z

[6] Anand P, Hameed P, Won-Hwa H, Hyun S, Seungmin R, Fog computing-based IoT for health monitoring system, Journal of Sensors, 2018, vol. 2018, Article ID 1386470, 7 pages, https://doi.org/10.1155/2018/1386470

[7] Michele D, Koen T, Nicola D, Foundations and evolution of modern computing paradigms: cloud, IoT, edge, and fog, IEEE Access, 2019, vol. 7, pp. 150936-150948, doi: 10.1109/ACCESS.2019.2947652

[8] Aazam M, Huh E, Fog computing and smart gateway based communication for cloud of things, 2014 International Conference on Future Internet of Things and Cloud, Barcelona, 2014, pp. 464-470, doi: 10.1109/FiCloud.2014.83

[9] Lee K, Kim D, Ha D, Rajput U, Oh H, On security and privacy issues of fog computing supported internet of things environment, 2015 6th International Conference on the Network of the Future (NOF), Montreal, QC, 2015, pp. 1-3, doi: 10.1109/NOF.2015.7333287

[10] Chen Y, Chang Y, Chen C, Lin Y, Chen J, Chang Y, Cloud-fog computing for information-centric internet-of-things applications, 2017 International Conference on Applied System Innovation (ICASI), Sapporo, 2017, pp. 637-640, doi: 10.1109/ICASI.2017.7988506

[11] Elazhary H, Internet of things (IoT), mobile cloud, cloudlet, mobile IoT, IoT cloud, fog, mobile edge, and edge emerging computing paradigms: disambiguation and research directions, Journal of Network and Computer Applications, 2019, Volume 128, Pages 105-140, ISSN 1084-8045

[12] Potluri S, Achyuth S, Elham Y, Mohanty S N, IOT enabled cloud based healthcare system using fog computing: a case study, Journal of Critical Reviews, ISSN- 2394-5125, 2020, Vol 7, Issue 6, PP: 1068-1072, doi: 10.31838/jcr.07.06.186

[13] Xuan-Qui P, Eui-Nam H, Towards task scheduling in a cloud-fog computing system, 2016 18th Asia-Pacific Network Operations and Management Symposium (APNOMS), Kanazawa, 2016, pp. 1-4, doi: 10.1109/APNOMS.2016.7737240

[14] Potluri S, Subbarao K, Improved quality of service-based cloud service ranking and recommendation model, TELKOMNIKA Telecommunication, Computing, Electronics and Control, 2020, Vol. 18, No. 3, pp. 1252~1258, ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018 DOI: 10.12928/TELKOMNIKA.v18i3.11915

[15] Potluri S, Subbarao K, A hybrid PSO based task selection and recommended system for cloud data, Test Engineering and Management, 2020, Vol-83, ISSN: 0193-4120, PP: 10210 – 10217

[16] Potluri S, Subbarao K, Hybrid self-adaptive PSO and QoS based machine learning model for cloud service data, International Journal of Control and Automation, 2020, Vol. 13, No. 2s, pp. 36 - 50, ISSN: 2005- 4297

[17] Binh M, Huynh T, Thanh B, Bao D, Evolutionary algorithms to optimize task scheduling problem for the IoT based bag-of-tasks application in cloud–fog computing environment, Appl. Sci, 2019, 9, 1730, https://doi.org/10.3390/app9091730

[18] Goiuri P, Iglesias-Urkia M, Barcelo M, Gomez R, Moran A, Bilbao J, Fog computing based efficient IoT scheme for the industry 4.0, 2017 IEEE International Workshop of Electronics, Control, Measurement, Signals and their Application to Mechatronics (ECMSM), Donostia-San Sebastian, 2017, pp. 1-6, doi: 10.1109/ECMSM.2017.7945879

[19] Yi S, Qin Z, Li Q, Security and privacy issues of fog computing: a survey, Xu K, Zhu H, Wireless Algorithms, Systems, and Applications, WASA 2015, Lecture Notes in Computer Science, 2015, vol 9204. Springer, Cham, https://doi.org/10.1007/978-3-319-21837-3_67

[20] Alrawais A, Alhothaily A, Hu C, Cheng X, Fog computing for the internet of things: security and privacy issues, IEEE Internet Computing, 2017, vol. 21, no. 2, pp. 34-42, doi: 10.1109/MIC.2017.37

Srikanth Pothuri

Marketing analytics as a Service: Secure Cloud Based Automation Strategy

Abstract: Efficient marketing strategies for business to business marketing (content, inbound, social media, SEO, SEM, account based, earned media, referral programs, industry events, conversational and step ahead as resolutions) and business to customer marketing (social network, paid media, internet, email, direct, point of purchase, cause, conversational, earned media and storytelling) are greatly heightened by using cloud based marketing automation solutions. Cloud governance ensure to meet business desires and needs through professional practices. Significant factors to ensure security in cloud marketing are embedded in each phase of marketing life cycle. Various cloud based secure marketing solutions are detailed and their performance is compared and illustrated in this work. To meet next generation marketing needs cloud based solutions are foremost preference for implementing efficient marketing strategies.

Keywords: Customer Relationship Management, Cloud Marketing, Marketing analytics as a Service, Cloud Security, Cloud Privacy

1 Introduction

Cloud based efficient solutions in marketing, sales, promotion and CRM saves money by converting capital expenses or capital expense (CapEx) into operating expenses or operating expenditure (OpEx). Flexibility, availability and ease of use features of cloud based marketing automation suite provides public cloud services based on pay as you use model to avoid investing on servers, storage devices and other computing infrastructure. For storing sensitive data, maintaining greater flexibility, security, privacy and control, the private cloud offers necessary business solutions. Hybrid cloud aimed at combining public and private clouds to meet the business objectives. To bring business groups or organizations together which are having common business interest, concern or goal in order to share CapEx and OpEx and observe reduced costs, community cloud is an abundant choice [1-3]. Various categories of clouds which are available to meet business objectives of diverse forms of organizations is given in fig. 1.

Srikanth Pothuri, Research Scholar, ICFAI Business School, ICFAI University Dehradun, Dehradun, Uttarakhand 248197, India, pothurisrikanth3@gmail.com

https://doi.org/10.1515/9783110732573-006

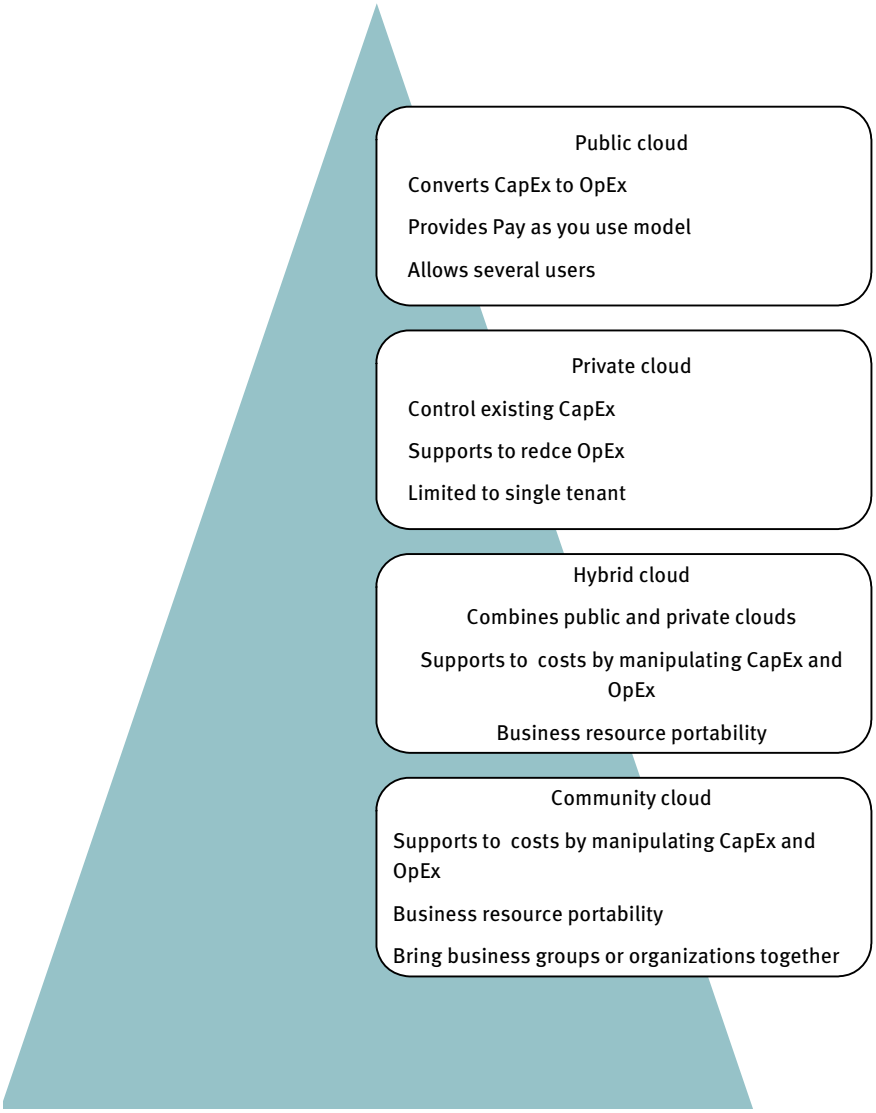

Fig. 1: Cloud deployment models for business and management

2 Cloud Governance through Marketing Automation: To Meet Business Desires

Cloud platform provides expert governance solutions to meet business needs, objectives and desires as shown in fig. 2. Marketing strategy includes the plan as given below.

- Identify: Ask yourself -Who you are and what you are for
- SWOT: Examine yourself- What are your strengths, weaknesses, opportunities, limitations
- Target- Identify yourself- Who is your target market, their behaviour and needs
- Inspection- Examine yourself- Where your target and your contributions intersect
- USP- Create yourself- What is your unique selling point
- Refine- Review yourself- what is your feedback and corrective measures

Fig. 2: Cloud governance solutions for efficient marketing strategies

Cloud governance lets your organization to bring everything together to satisfy various business needs: business monitoring, recommendations, operations management, cost transparency, cost optimization, scheduled policies, lead dashboard, lead analytics, report generation, auditing, budget management, and security and compliance governance. The major disciplines cloud governance are shown in fig. 3.

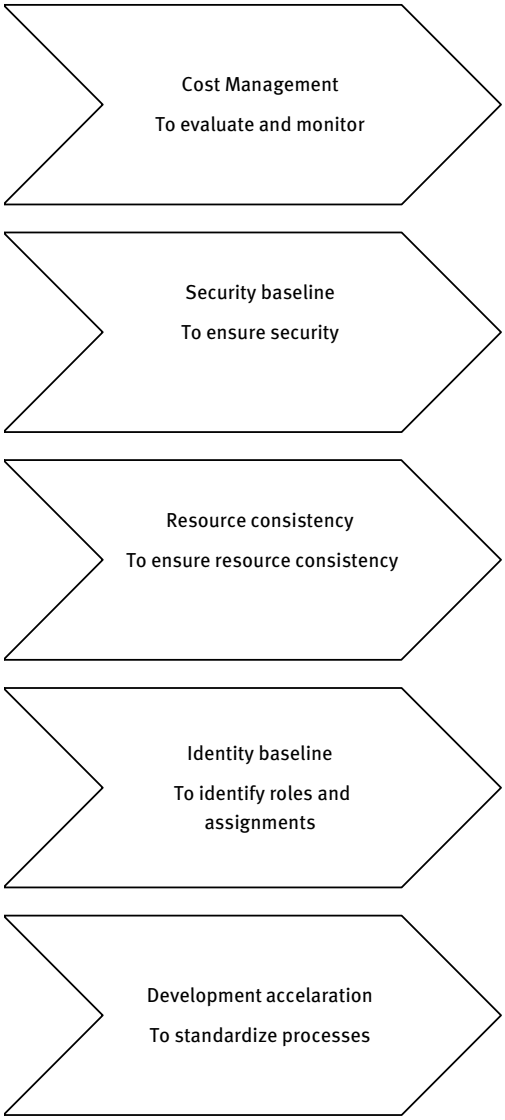

Fig. 3: Major disciplines of cloud governance

3 Significant Factors Ensuring Security in Cloud Based Marketing Automation Process

The three main areas of security concerns in the cloud-based applications are access, data, and platform [4-6]. Let us examine these in detail.

3.1 Access security

Cloud offers an integrated data storage, computing and networking mechanism. "Who can access the data" is firmly administered by having access rights. SaaS providers add additional layer of security and privacy to stop unauthorized access to information in cloud.

3.2 Data security

Recent applications need infrastructure for data security to meet ongoing business demands and needs. The increasing need of data storage, data processing and data analytics on the cloud, has also improved the need and responsibility of data security on cloud service providers.

3.3 Platform security

A cloud platform is a physical system that offers, houses and distributes information. Cloud platform delivers an on-demand platform and environment for designing, developing, challenging, delivering, and handling software applications.

Significance factors ensuring security in cloud based marketing automation process at a glance is given in fig. 4.

4 Automation of Marketing Life Cycle Through Cloud Based Secure Marketing Solution

The practical framework, RACE (Reach, Act, Convert, and Engage) can be automated through cloud based secure marketing solutions [7-10].

The RACE Framework consists of these four steps and online marketing activities are designed to help marketing people to engage their customers throughout the customer lifecycle. The framework is demonstrated in fig. 5.

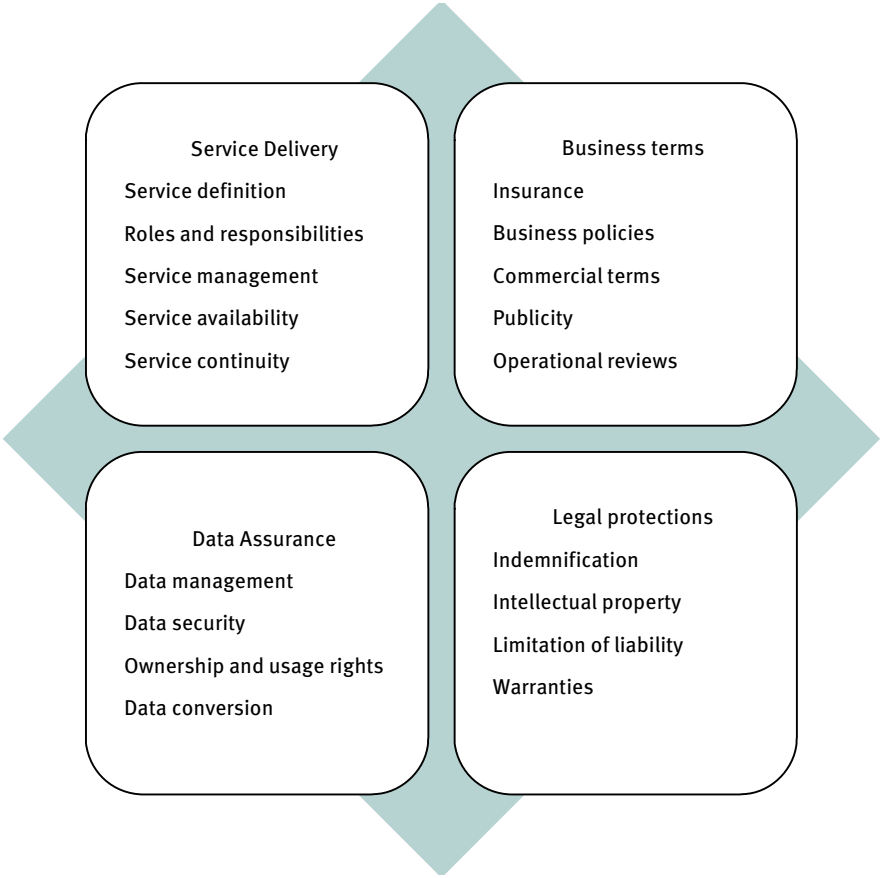

Fig. 4: Significance factors ensuring security in cloud based marketing automation process

4.1 Reach

Reach includes building product awareness, media usage and visibility through messaging, live chat, website visits, social media posts, advertising and mouth publicity. It ensures maximizing the reach over time of the customer by creating several interactions using different ways of paid, unpaid, owned, public and earned media networks and touchpoints. This is to bring awareness of a particular brand or product.

4.2 Act

It is a short form of interact. With interest and intent, sales team get leads through conversations, chat, booked calls, webinars, email marketing, list building and

more other means of interaction. For many categories of businesses, particularly, B-to-B, this step can bring decent quantity of leads.

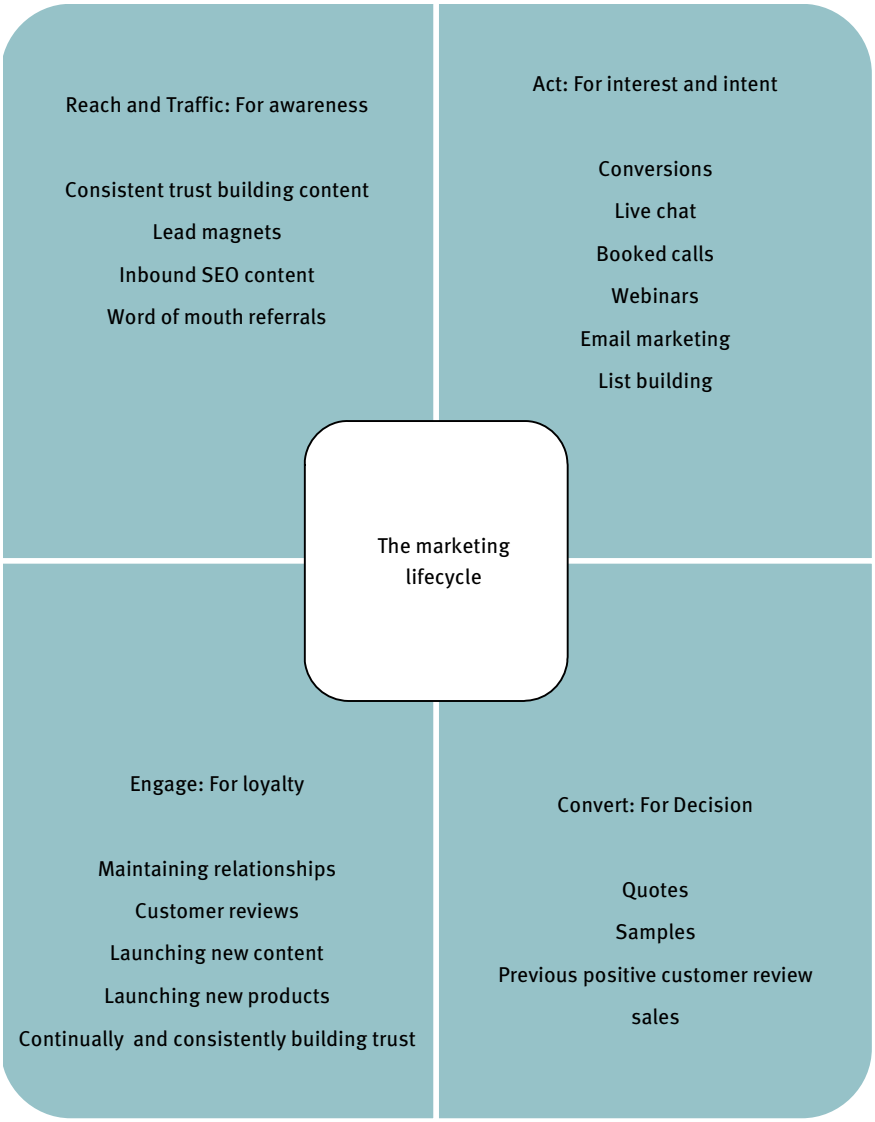

Fig. 5: The marketing life cycle- RACE framework

4.3 Convert

This step ensures online or offline lead conversion to sale. It includes getting your target audience and customers to take the next important step of payment through online transaction, ecommerce or offline modes. This step uses product quotes, product samples, previous positive customer reviews and sales information to engage the customer.

4.4 Engage

This is a long-term commitment and engagement, evolving a long-term association and relationship with initial and first-time product buyers to form customer loyalty as recurrence and repeat product purchases. Engage is ensured by using communications on your web site, social network posts and active presence, email interactions, direct communications and messaging. Loyalty of the customer is maintained through healthy relationships, competent reviews, launching new products, continuous positive feedback and consistently building trust.

5 Various Cloud Based Secure Marketing Solutions

5.1 Adzooma software

Adzooma is a digital publicity and advertising platform that supports and benefits businesses of all dimensions of the organizations to expand marketing related operations and strategies by improving and optimizing sales promotions across Google marketing platform, Facebook influencer marketing platform and Microsoft marketing and advertising center. Using the opportunity engine platform and machine/deep learning processes, experts can view programmed and automated recommendations about recommended keywords, smart targeting, budget and economy management, CRO- conversion rate optimization and LPO- landing page optimization.

Organizations are using Adzooma to study and analyze recommended data and inevitably break in proceedings for ongoing promotions or proposals on low performing keywords. Marketing managers can constitute automation rules by outlining precise conditions and situations to obtain reports about the budget which is overspend across promotions. Furthermore, it lets cloud users manage several accounts on a centralized environment and filter account particulars by date sort.

Marketing hierarchies can use Adzooma for customizable analysis and collect stakeholders. Pricing is based on periodic basis (say monthly) subscriptions and

payments are extended via feedback, live chat, email, slack, phone and other online or accessible processes.

5.2 Bitrix24 software

Bitrix24 is a client or customer supervising solution that offers the infrastructure and platform for businesses to establish and track relations with potential and prospective customers and partners. Using this software, users maintain and manage log of interactions to capture and pile lead data, produce sales reports and accomplish breakdown of target audiences. Leads which are received from a source can be fed directly as an entry to the CRM, create message template, sending communication to leads, identify potential communication to interact with clients and schedule meetings to meet targets. Users can produce custom-made statements for clients by automatically maintaining the client information and sending the same to them through email.

Bitrix24's sales funnel module offers an overview of sales communications and transactions. With the sales control panel/dashboard, sales managers can see the comparison of deals, rating and sales of all team members.

5.3 WebEngage software

WebEngage is a customer relationship management platform provides marketing automation, customer data management, user engagement and maintenance not only for large sized business organizations but also SMBs. WebEngage sales control panel/dashboard allows to identify potential customers, aim for better client interactions, marketing analytics, fixing campaign calendar and tracking growth metrics for great journey towards healthy targets.

This software has wide range of use across the globe for various domains such as ecommerce, education, marketing analytics, business services, social media, healthcare, retail, manufacturing, gaming, banking, Financial Services and Insurance (BFSI) and many more.

5.4 BetterMetrics software

BetterMetrics is a resolution in marketing domain using which report automation, next generation digital marketing using pay-per-click (PPC) strategy and integration with various ongoing and on demand data management applications such as Google sheets (Google analytics), Data Studio (Google interactive dashboard) and Big Query (cloud data warehouse) solution that enables digital marketers to gather and aggregate all their PPC data in a centralized location. This software is available on pay per

use model (subscription based- monthly). Advantages of this software are mining for better metrics for users unified reporting and comprehensive examination.

5.5 EngageBay software

EngageBay is a combined solution for various domains such as marketing, sales, promotion and CRM. This software mainly meant and designed for SMBs to obtain, absorb and transform website visitors into prospective customers. This cloud-based software allows business organizations to use this as a marketing tool to construct healthy relationships with customers and preserve them for long time.

Advantages of EngageBay are email marketing (for communication), landing pages (for optimization), live chat/helpdesk (for engaging), ticketing (for announcing), telephony (for broadcasting), appointment scheduling (for publicizing), contact management (for spreading) and more. It has eminent features namely built-in CRM support, marketing capabilities, lead conversion policies, email templates, social media visibility, forms and popups for better communication and automated mails and communication.

5.6 Agile CRM software

Agile CRM is a cloud enabled CRM resolution designed for SMBs. It deals contact supervision, telephony techniques, appointment arranging, marketing process automation, project organization, landing-page designer and knowledge and information base functionalities.

This software also provides email services by integrating and syncing data with Gmail, Yahoo, Microsoft Exchange, Hotmail, Office 365 and IMAP. Users can analyze about website visitors to study customer conduct, marketing automation procedures, task management and generate marketing process flow with GUI interface. Using user friendly GUI, task management ended up in easy manner through dragging, dropping, sorting, adding, and updating tasks or task status. Social media collaboration is made feasible through integrating with Facebook, Twitter, Instagram, Tumblr, WeChat, Messenger, LinkedIn and many more.

5.7 Sender software

Sender is a cloud enabled email marketing, advertising and sales solution that supports users to generate and handle email-based promotions advertisements for SMBs. Significant features of sender software contain customizable subscription procedures and prototypes, subscriber partitioning and management tools, email customization and management, third-party incorporations and more.

Users can send advertising and promotional emails, all-purpose surveys or newssheets based on customizable prototypes. Sender also offers plugins for third-party payment and e-commerce platforms that allow organizations to pull customer data for emails and integrate product information to newssheets. Users can supplement multimedia files such as images in various formats, audio, video and animated and dynamic GIFs. Pricing is based on periodic basis (say monthly) subscriptions and payments are extended via feedback through smart phone and email.

5.8 SendX software

SendX is an In-built, reasonable & customizable email marketing, advertising and sales software for all stakeholders of the organization. It allows users to send unrestricted email promotions, construct email comprehensions, GUI based design of emails with drag and drop features, email sequence, customization and automation. This software ensures 24x7 active and live support and maintenance, better migration services, customizable and responsive email prototypes and image repository for email promotions and campaigns. Pricing is based on periodic basis (say monthly and yearly) subscriptions and payments are extended via feedback through email and live chat.

5.9 InTouch software

InTouch software is a browser (Chrome) extension service to automate LinkedIn communications and messages. It is a safest and perfect tool for perfect for lead generation, monitoring sales and sales management in LinkedIn. This software prospects LinkedIn by automating the process through auto connect or join mass scale messaging, scraper and lead board customization.

Auto connect or join mass scale messaging provides customized message management, flexible message sending and follow up. Scraper is used to define target customers through social media network. Lead board customization provides dashboard to start, view or manage your leads through tasks. InTouch software is used by marketing professionals, business vendors, service provider, and recruiters.

5.10 SendinBlue

SendinBlue is a cloud enabled email based marketing, advertising and promotion tool suited for large, medium and small size organizations. It offers automation of marketing advertising and sales, email promotions, log of transactional emails and customized free range SMS messages functionalities within a package.

SendinBlue lets users to produce, schedule, automate or deliver mobile based responsive and dynamic emails using customization tools and APIs. This software has rich customer communication management through introducing contacts, classifying and grouping lists, collecting and designing forms, communicative forms and many more. SendinBlue allows reporting, content management, e-commerce administration, exporting and importing results and responsive website management.

5.11 Freshworks CRM software

Freshworks CRM is a cloud enabled efficient customer relationship management solution that helps organizations through diverse business verticals to accomplish their communications with prevailing and prospective customers.

Significant features consist of sales tracking, sales management, event management, single click phone and task administration. Users can also refer custom-made majority emails from the proposed solution, and then monitor accomplishments on these email activities. The inbox spontaneously highlights emails from contacts, connections and leads that are coming up for an active response. Freshworks CRM trails for the dynamic and responsive web pages that prospects the contacts behavior, lead board dashboard generation, task prioritization, customers and their lead management, including discussions, touch points, activities, appointments, and responsibilities.

5.12 Routee software

Routee is a cloud-based tool intended to help business organizations of large, medium and small scale. It provides process flow of message based marketing, lead generation, bulk messaging, double-factor verification, push announcements, real-time broadcasting and data analytics.

Routee lets business organizations to send custom-made mass produced messages to the customers by including essential information. This tool enables users to generate promotions, track communications and connections, produce subscription practices, target and segment leads through several channels and systems.

5.13 Zoho CRM software

Zoho CRM is a cloud enabled business management and administration tool that helps business organizations of large, medium and small scale. It deals sales, advertising and marketing automation software with dashboard and helpdesk, data analytics, data visualization and customer support utilities.

It has artificial intelligence powered sales assistant for strong customer relationship management, data indicators, dynamic statistics and well-organized integration to third parties such as Google Suite, WordPress API, MailChimp automation tool, Evernote App and Unbounce.

5.14 Omnisend software

Omnisend is an efficient marketing, advertising and sales automation platform for development concentrated ecommerce based business organizations. This software permits you to enhance several networks to the same automation process flow for unified communication via tools like email, messaging, live chat, web push notifications and announcements, and customer base management.

This can produce strong automation process flows and customize your message and communication based on customer record, campaign arrangement and recommendations through shopping behavior. Omnisend provides integration with the popularity of ecommerce applications platforms and other marketing management tools. Pricing is based on periodic basis (say monthly) subscriptions and payments are extended via feedback through smart phone, live chat, knowledge sharing and email.

5.15 AiHello software

AiHello software is mainly aimed for Amazon pay-per-click (PPC) operations and promotions. It has significant modules, auto pilot (for efficient ecommerce marketing, advertising and sales) tool, bidding optimization (for pay-per-click based top-notch automation and bidding) tool, Artificial intelligence engine (for intelligent business automation), advanced algorithms library (for restocking support and sales forecasting), real-time analytics (for examining and analysing customer activities periodically), multichannel analytics (for integrating easily with different date sources, warehouses and applications such as Shopify, Woocommerce, and Magento), ecommerce application (to support connection with various ecommerce platforms) and marketing analytics (for information management).

5.16 Mailchimp software

MailChimp is a cloud and web-based email marketing, advertising and sales automation service with millions of global users. The tools lets users to share newssheets or letters on several social networks to examine and track the customer behavior and engagements. This tool offers customer targeted emails, run Facebook ad promotions and campaigns, systematize follow-ups and observe promotion and campaign activities development and progress and many more.

Using this tool, users can gather and evaluate their email replies. The application offers an efficient GUI support for graphical representations and demonstrations of data and customer connections/communications in various formats. MailChimp lets users to plan, share and identify email newssheets and letters from any location all over the world. This tool provides interactive user friendly drag & drop graphical user interface, data analytics tools, customized report generation, mobile based application support for Android and iOS, customer relationship management, social media activity subscription, campaign management and ecommerce based retail marketing. Pricing is based on periodic basis (say monthly and yearly) subscriptions and payments are extended via feedback through email and live chat.

5.17 HubSpot Marketing Hub software

HubSpot is a prominent cloud based advanced platform. Marketing Hub supports companies for their web presence for lead generation, analyze return on investment (ROI), marketing hub for business to business and business to customer service, software utilities and libraries for marketing automation, state of the art technologies, accounting packages, construction strategies, retail business policies, real estate approaches and more.

This software provides various solutions to invite more visitors, adapt more leads, accomplish more deals and finally satisfy more customers. It has integrated blogging tools, and content design tools, SEO optimization, lead conversion techniques, construction of landing pages, call to action (CTA) tools, live chat and world class state of the art marketing automation. It has a powerful hub to automate marketing, sales, service, CRM and other essential organization related strategies.

5.18 Constant Contact software

Constant Contact offers a variety of in-built marketing automation applications intended to assist small business organizations and nonprofit organizations to develop their customer bases and cherish customer relationships. This tool has email and event marketing, social promotions and events, and event reporting, survey/review/assessment management and bid management.

Constant Contact permits business organizations for customer relationship management using spreadsheets, emails, messages, web forms, web activities, contacts, social media activities and other customer related activities. Constant Contact deals both online and offline customer engagement activities through seminars, training, interactive programs and other campaigns.

5.19 Wrike software

Wrike is a cloud enabled business management and administration tool that helps business organizations of large, medium and small scale. It provisions remote work for all marketing verticals through Gantt charts, event calendars, workload balance sheets, efficient resource management, custom control panel and dashboards, and real-time analytics. This software provides hierarchical structuring through files, folders, events, projects, modules, jobs and tasks. It has custom made templates, libraries, extensions, tools, integrations (Salesforce, LinkedIn, Dropbox, Google suite, Slack, facebook and Adobe Creative Cloud) API for efficient marketing, advertising and sales automation platform. Pricing is based on periodic basis (say monthly and yearly) subscriptions and payments are extended via feedback through email and live chat.

5.20 Semrush software

SEMrush is an efficient marketing, advertising and sales automation solution aimed to benefit organizations and enterprises streamline the processes associated to keyword based research, search engine optimization, advertising promotions and activities, sales monitoring and more. Marketing professionals can observe improvement in their domains through this tool with improved traffic, movement, keyword classification and ranking, keyword usage metrics, organic research tool, content management strategies.

SEMrush allows organizations and businesses to study the responsiveness of website content across various social networking sites and accordingly release posts across Facebook, Twitter, Instagram, Tumblr, WeChat, Messenger, LinkedIn and many more.

On a scale of 1-5 the impressions of various marketing solutions are captured for different parameters. Recommendation is a label from a set of labels [“not recommended”, “likely recommended”, “more likely recommended”, “highly recommended”]. Analysis is displayed in table 1.

Tab. 1: Comparison of various cloud based marketing solutions

S.No	Software	Overall rating	Ease of use	Value for money	Customer support	Functionality	Recommendation
1	Adzooma	4.18	4.5	4.5	4.5	4.0	Likely recommended
2	Bitrix24 Software	4.0	4.0	5.0	3.0	4.0	Likely recommended

S.No	Software	Overall rating	Ease of use	Value for money	Customer support	Functionality	Recommendation
3	WebEngage	4.0	4.0	5.0	4.0	4.0	Likely recommended
4	BetterMetrics	4.2	5.0	5.0	4.5	4.0	More likely recommended
5	EngageBay	4.63	4.5	5.0	5.0	4.5	Highly recommended
6	Agile CRM	4.12	4.0	5.0	3.5	5.0	Likely recommended
7	Sender	4.6	5.0	5.0	5.0	4.5	Highly recommended
8	SendX	4.74	4.5	4.5	4.5	4.5	Highly recommended
9	InTouch	4.88	5.0	5.0	5.0	5.0	Highly recommended
10	SendinBlue	4.59	4.5	4.5	4.5	4.5	Highly recommended
11	Freshworks CRM	4.62	4.5	4.5	4.5	4.5	Highly recommended
12	Routee	4.3	4.0	4.0	4.5	4.0	More likely recommended
13	Zoho CRM	4.2	4.0	4.0	4.5	4.5	More likely recommended
14	Omnisend	4.77	4.5	4.5	4.5	4.5	Highly recommended
15	AiHello	4.6	4.0	5.0	5.0	5.0	Highly recommended
16	MailChimp	4.48	4.5	4.5	4.0	5.0	More likely recommended
17	HubSpot Marketing Hub	4.49	4.5	4.0	4.5	4.5	More likely recommended
18	Constant Contact	4.0	4.0	4.0	4.0	4.0	Likely recommended
19	Wrike	4.28	4.0	4.0	4.5	4.0	More likely recommended
20	SEMrush	4.65	4.5	4.5	4.8	4.9	Highly recommended

Comparison of various cloud based marketing solutions are shown in fig. 6.

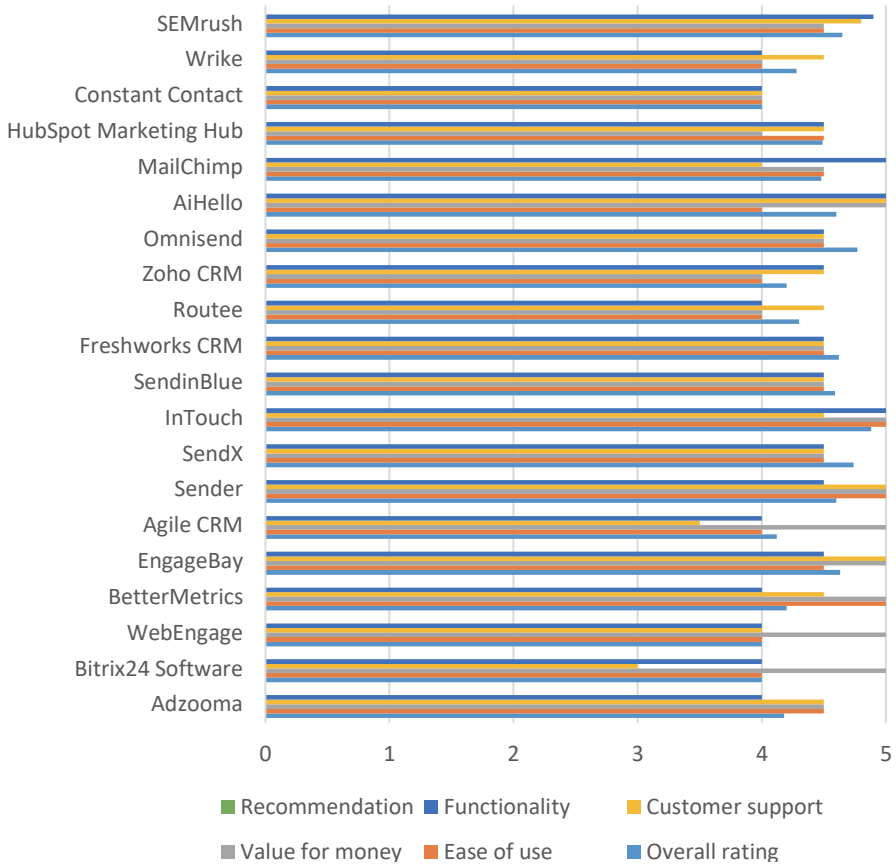

Fig. 6: Analysis of various cloud based secure marketing solutions

Comparison of the given cloud based marketing models on their overall rating and recommendation label is given in fig. 7.

6 Results and Discussion

All these cloud solutions for best practices in marketing are revealing the following.

- Stand out by accepting, understanding and appreciating your customers
- Improve the focus and concentration of your marketing team to look up the full context and perspective of customer requirements and demands

- Engage and participate with seamless, continuous and personalised experiences and understandings
- Automate RACE framework for reach, act, convert and engage
- Ensure security across marketing activities through secure cloud based marketing software/tools
- Guarantee cloud governance in marketing verticals to observe efficient cost management, resource usage and development
- Build customer expectation and trust
- Extend customer relationships and associations with greater perception and agility
- Accomplish your assurances to customers and the product/brand
- Use real-time business computation and intelligence to empower fast data analysis
- Use cloud based marketing automation to assure dynamic and flexible decision-making across the organisation
- Delight customers through optimising marketing presentation
- Observe demand and development for B2B marketing with cloud based marketing automation tools
- Empower marketers to productively generate potential lead conversions, and, eventually, drive more business
- Create a business test case to promote your marketing practices and strategies
- Apply "customer first" strategy
- Obtain efficient cloud based solution to create modern multichannel marketing
- Perceive efficient and easy marketing management with efficient SEO tools built on real-time data
- Complete and in-built marketing segmentation functions and verticals
- Custom-made communication
- Real-time data analytics on customers data for quick and effective decision making
- Dynamic generation of customer profiles across all networks can be analyzed identify their behavior and requirements
- Lead Management functions integrated to marketing and sales departments for cross-departmental analysis
- Identify organization needs and can deploy a cloud type: public, private, hybrid or community
- Identify marketing needs and requirements and get the service as marketing analytics as a service form the cloud service provider
- Identify integration of various departments in an organization and same can be perceived by using cloud based marketing software
- Enable personal, associated journeys that will increase customer conversion
- Drive loyalty and escalate marketing's contribution and involvement to the bottom line

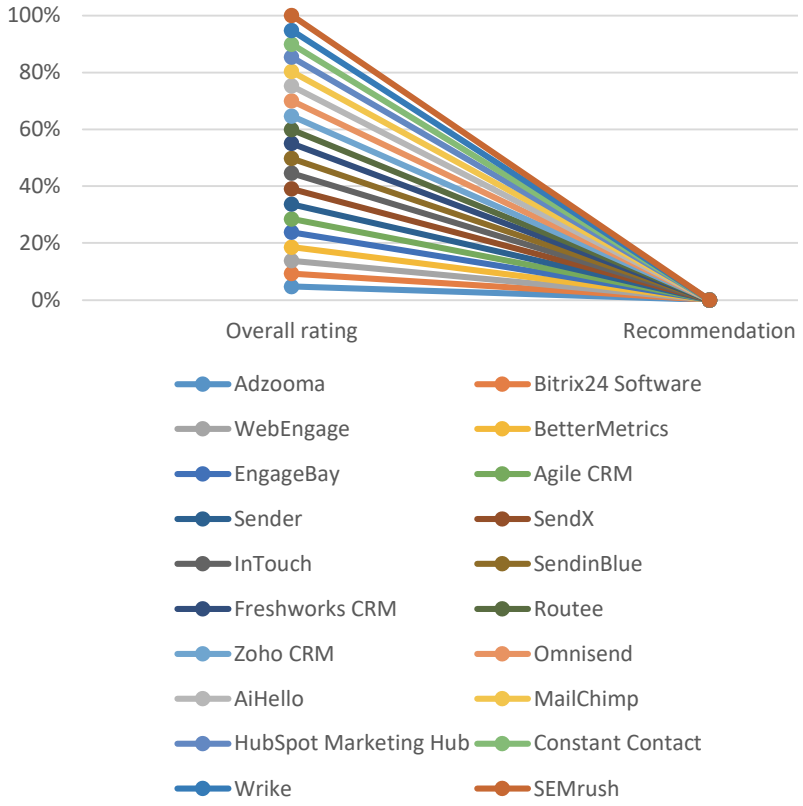

Fig. 7: Comparison of the given cloud based marketing models based on their over-all rating and recommendation

7 Conclusion

There are various other cloud based marketing tools such as Sap Marketing Cloud, Lengow, Basis, ZoomInfo, Evocalize, Jilt, FIREBusinessPlatform, Promoboxx, Adsale, Influx MD, MailOptin, Involve.me, FunnelMaker, Converttri, Privy, Oracle Datamanagement Platform, SutiCRM, Automizy, Morph.ai, SlickText, Vitalblocks CRM, Synerise, Goody, MoonMail, EmailDelivery.com, Tabrasa, TractionNext, Whatagraph, Texting Base, TargetEveryone, SugarCRM, SendPulse, SalesSeek, Skyword, Rejoiner, Pure360, Prisync, QZZR, Post Planner, Voogy, Mission Suite, iSalesCRM, marketing Automation Professional, Marketing Automation Enterprise, BOTNATION AI, Mailify, LeadByte, Blackbaud Luminate Online, Instapage, Intercom, Greenrope, Genoo, Higher Logic, FreshMail, EverString, Ecrion, Dialog Insight, AutoManager, ConvergeHub, Contactually, Click2Mail, ConnectAndSell, ClickDi-

mensions, Brightpod, C2CRM, Bronto Marketing Platform, BigMarker, BannerFlow, PromoNavi, Salesgenie, Bonzo, Nimbus Omnichannel, Insightly Marketing, BounceX, INBOX25 and many more. Marketing life cycle yields more production with using these efficient cloud based tool by implementing best practices.

8 References

[1] Kirtiş K, Karahan F, To be or not to be in social media arena as the most cost-efficient marketing strategy after the global recession, Procedia - Social and Behavioral Sciences, 2011, Volume 24, Pages 260-268, ISSN 1877-0428, https://doi.org/10.1016/j.sbspro.2011.09.083

[2] Muliana M, Nek K, Azhari A, An overview of private preschool in malaysia: marketing strategies and challenges, Procedia - Social and Behavioral Sciences, 2014, Volume 130, Pages 105-113, ISSN 1877-0428, https://doi.org/10.1016/j.sbspro.2014.04.013

[3] Joseph J, Jeffery S, Mark R, Ramirez E, Martinez J, Green marketing strategies: an examination of stakeholders and the opportunities they present, J. of the Acad. Mark. Sci, 2011, 39, 158–174, https://doi.org/10.1007/s11747-010-0227-0

[4] Nancy W, Innovative marketing strategies in academic libraries: an overview, innovations in the designing and marketing of information services, Jeyasekar J, Saravanan P, IGI Global, 2020, pp. 1-15. http://doi:10.4018/978-1-7998-1482-5.ch001

[5] John P, Steven M, Marketing strategies that make entrepreneurial firms recession-resistant, Journal of Business Venturing, 1997, Volume 12, Issue 4, Pages 301-314, ISSN 0883-9026, https://doi.org/10.1016/S0883-9026(97)89449-9

[6] Baena V, Online and mobile marketing strategies as drivers of brand love in sports teams: findings from real madrid, International Journal of Sports Marketing and Sponsorship, 2016, Vol. 17, No. 3, pp. 202-218, https://doi.org/10.1108/IJSMS-08-2016-015

[7] Aspelund A, Madsen K, Moen, A review of the foundation, international marketing strategies, and performance of international new ventures, European Journal of Marketing, 2007, Vol. 41 No. 11/12, pp. 1423-1448, https://doi.org/10.1108/03090560710821242

[8] Gabrielsson P, Gabrielsson M, Seppälä T, Marketing strategies for foreign expansion of companies originating in small and open economies: the consequences of strategic fit and performance, Journal of International Marketing, 2012, 20(2), 25–48, https://doi.org/10.1509/jim.11.0068

[9] Cacciolatti L, Hee S, Revisiting the relationship between marketing capabilities and firm performance: the moderating role of market orientation, marketing strategy and organisational power, Journal of Business Research, 2016, Volume 69, Issue 12, Pages 5597-5610, ISSN 0148-2963, https://doi.org/10.1016/j.jbusres.2016.03.067

[10] Adjei M, Clark M, Relationship marketing in a B2C context: the moderating role of personality traits, Journal of Retailing and Consumer Services, 2010, Volume 17, Issue 1, Pages 73-79, ISSN 0969-6989, https://doi.org/10.1016/j.jretconser.2009.10.001

Sachi Nandan Mohanty, Gouse Baig Mohammad, Sirisha Potluri,
P. Ramya, P. Lavanya

Next Generation Cloud Security: State of the Art Machine Learning Model

Abstract: Recent days have seen an obvious shift in computing platforms and environments with the arrival of cloud computing. Most of the organizations moving towards cloud technology to satisfy varied user demands and requests, and to guard and safeguard the transactions and operations of the organizations. Over the cloud platforms, it is extremely essential to produce a secure and strong environmental support to ensure security and privacy. Machine learning (ML) based models have well-tried their significance to anticipate in finest outcomes to boost the choice of cloud based long-term course of actions. Efficient machine learning models have long been utilized in several application domains that required the identification and prioritization of adverse factors for a threat. The main objective of this paper is to propose a best strategic cloud security enhancement model for next generation computing standards. Efficient machine learning algorithms like convolution neural network gives automatic and responsive approaches to reinforce security in a cloud environment. These models give solutions that incorporate holistic approaches for secure enterprise knowledge throughout all the cloud applications.

Keywords: Machine Learning, Cloud Security, Cloud Privacy, Cloud Computing

Sachi Nandan Mohanty, Department of Computer Engineering, College of Engineering Pune, Wellesley Rd, Shivajinagar, Pune, Maharashtra 411005, India, sachinandan09@gmail.com
Gouse Baig Mohammad, Department of CSE, Vardhaman College of Engineering, Hyderabad, Telangana 501218, India, gousebaig@vardhaman.org
Sirisha Potluri, Department of CSE, IcfaiTech (Faculty of Science and Technology), ICFAI Foundation for Higher Education, Donthanapally, Shankarpalli Road, Hyderabad, Telangana 501203, India, sirisha.vegunta@gmail.com
Ramya Reddy Padala, Department of CSE, IcfaiTech (Faculty of Science and Technology), ICFAI Foundation for Higher Education, Donthanapally, Shankarapalli Road, Hyderabad, Telangana 501203, India, ramyapadala28@gmail.com
Lavanya Reddy Padala, Department of CSE, IcfaiTech (Faculty of Science and Technology), ICFAI Foundation for Higher Education, Donthanapally, Shankarapalli Road, Hyderabad, Telangana 501203, India, lavanyapadala5@gmail.com

https://doi.org/10.1515/9783110732573-007

1 Introduction

1.1 Cloud computing

Cloud computing is a new distributed and computing technology using which we can achieve enhancement in the use of virtualized resources. These virtualized resources are designed for the service provisioning of the end users in the dynamic cloud environment in order to provide reliable and trusted services to cloud users all the time. The main advantage of cloud computing environment is that we can improve and optimize the utilization of physical resources as much as possible. The beauty of this technology mainly lies by applying abstraction and isolation of physical resources so as to reduce the requirement of the hardware equipment. To handle the dynamic tasks which are highly based on the demand, the cloud computing is making use of virtualization. Virtualization is the technology using which many virtual machines for a given single physical resource/server can be created to handle/execute the multiple tasks. Resource management plays an important and vital role here because of this dynamic provisioning of the resources to handle the on demand service requirement of the cloud computing environment. The main objectives of the resource management are to maximize the utilization time of resources, to reduce the task execution time, to achieve high system throughput and to improve load balancing. In any cloud system architecture mainly there are three main modules namely application (source for task submission), mapping algorithms (uses various algorithms to map the submitted tasks to physical resources) and virtual machine. Using mapping algorithms a set of cloudlets are mapped to resources by estimating the expected time of completion of cloudlets and then execute the cloudlets on selected resources [1-2].

1.2 Machine learning

Machine learning based systems were proved as best solutions to every alternative in far and wide. Foremost cloud service providers like Amazon internet services, Microsoft azure, and Google cloud implements machine learning for their enterprise level security. All major cloud service providers use totally different machine learning systems which are different from one another in terms of their functionality and hierarchy [3].

1.3 Advantages of machine learning systems on the cloud

The advantages of the machine learning systems on the cloud are summarized as below [4-5].

- Machine learning based cloud systems are price competent solutions
- Integration of machine learning models with computer program Interface(s) (APIs) and computer code developer kits (SDKs) is effortlessly well-suited
- Machine learning based cloud secure solutions has intelligent future and able demand
- Scalability is enhanced in pay per use model of cloud with machine learning based applications
- Machine learning based cloud applications provides enhanced cloud based solutions

1.4 Limitations of machine learning systems on cloud

The limitations of the machine learning systems on the cloud are summarized as below [6].

- Lack of specialized skill personnel and expertise due to insufficiency and absence of domain knowledge
- Limited support to accomplish information integration and attachment at enterprise level
- Increased deployment cost to achieve required computational power through infrastructure and workforce
- Basic engineering, easy and medium complex problems are addressed by using open source machine learning tools such as Tensor Flow, MXNet and CNTK. Whereas these models may not give efficient solutions for the problems with greater complexity and convolution

1.5 Literature survey

- B. Nassif et al. stated that the best way to ensure security in cloud is by using machine learning models. This paper summarizes about different types of cloud security threats, various machine learning techniques and performance related outcomes. According to the survey results, they stated that support vector machine model is one of the best machine learning technique, true positive rate and training time are the most applied and least applied metrics respectively, KDD and KDD CUP'99 are mostly used datasets [7].
- Han Qiu et al. stated that IoT based remote healthcare system uses cloud based data analytics to build body sensor network. To make certain security and privacy preservation in body sensor network cloud computing model is using selective encryption techniques through machine learning approach. Light weight selective encryption technique design is based on the efficient classification machine learning models [8].
- Sirisha Potluri et al. stated that detection and prevention mechanisms related to DDoS attacks in cloud necessitate efficient dynamic usage of the cloud resources. To handle these adverse effects, cloud uses various defence mechanisms using machine learning [9].

- H. Karimipour et al. stated that security threats and vulnerabilities in digital communication technology are addressed by using machine learning techniques for efficient and reliable power distribution. Symbolic dynamic filtering technique is used to reduce computational encumber in smart grids while discovering laid-back interactions among the nodes [10].
- Wei Wu et al. stated that unsupervised machine learning model is used for Bot detection during traffic analysis based on similarity measures. An efficient clustering algorithm is used to identify majority clusters with most flows, elimination of duplicate flows, and computation of similarity analysis [11].
- Ünal Çavuşoğlu et al. stated that hybrid and layered intrusion detection system uses a combination of various machine learning and feature selection techniques to provide high performance intrusion detection in different attack types [12].
- Sirisha Potluri et al. stated that fog computing network is designed for distributed and decentralized computing platform by using IoT infrastructure to send and receive the data. Various applications of fog computing includes e-commerce, mobile, agriculture, auto mobiles, smart grids, healthcare and data analytics [13].
- Mahmud et al. stated that fog-based IoT healthcare solution structure integrates cloud and fog based services in interoperable healthcare solutions. Using iFogSim simulator the results are analysed in view of distributed computing to show latency reduction, communication cost optimization and efficient energy consumption [14].
- Subramanian, E. et al. stated that with the aim of security and privacy to safeguard the cloud transactions, it is extremely necessary to provide a secure, safe and robust machine learning based solution across cloud vicinity. Various machine learning approaches such as linear regression, convolution neural network, and support vector machine provide enhanced cloud based solutions for ensuring security and privacy [15].
- Mbarek Marwan et al. stated that using support vector machines and fuzzy C-means clustering classification of image pixels can be done more efficiently. Using conventional two layered architecture, simultaneous image segmentation and data protection is achieved in medical image data [16].

2 Machine Learning Based Cloud Solutions to Address Research Issues and Challenges

2.1 Privacy and security aware safety measures

Cloud computing environment make use of large amounts of datasets for storage and processing. On premise data storage, handling, processing is completely risk free. But if the data is getting saved in other places there is a greater risk involved in

that. Cloud service providers, intermediaries or the companies involved in hosting of cloud platforms may disclose the data which is being in access to them. Due to which data may be tampered or lost. In either of the cases it leads to security and privacy issues. Due to these reasons of security and privacy, cloud computing is taking slightly a back step apart from its wider adoption. Machine learning based cloud computing models and approaches gives next generation privacy and security in computing platforms [17].

2.2 Performance and its measurement

In cloud environment, this issue is very much important as it is one of the measuring techniques in computing environment. Performance is a major concern in cloud system which affects the delivery of various services, revenue generated due to service delivery and the number of customers involved in the process [18].

2.3 Attentive solutions through reliability and availability

Reliability defines the certain expected functioning of the system under selected time interval and with given conditions. Availability of any system can be defined as degree in which the set of resources are available and these available resources are used whenever and wherever there is a need. These two factors comes together and defines the strength and potency of the system [19].

2.4 Accustomed solutions through scalability and elasticity

Scalability can be defined as its ability to adapt to the changes. When there is a need of resources by various cloud users, the system should take care of workloads efficiently. Elasticity of the system can be defined as the factor up to which it can handle the workloads efficiently. Elasticity ensures allocation and deallocation of resources to handle the needs of on demand users [20].

2.5 Adaptive solution through interoperability and portability

Interoperability of cloud computing environment can be defined as the power or ability which is adopted by the system to run various services which are from various vendors. Its associated factor interoperability can be defined as the way in which different platforms are effectively used among different cloud service providers. Portability is an important factor which defines the ability to transfer the related

data applications from one CSP to another CSP without much dependency involved in it [21].

2.6 QoS driven resource management and scheduling

Resource management can be defined as a factor which represents the efficient usage and maintenance of the resources. Various types of resources are mapped to the submitted jobs so as to schedule them in a more efficient manner. A better resource scheduling or provision can be achieved by using a better scheduling policy. By using these scheduling algorithms, we can optimize cloud services to achieve high level of quality of service. There are many categories of users, tasks and resources using which task mapping and execution is achieved [22-24].

2.7 Efficient energy consumption infrastructure

Any cloud data centre or storage consists of infrastructure in large and voluminous amounts. Cloud computing environment is delivering various types of services to enormous users by using its massive infrastructure. Cooling infrastructure is needed to compensate the heat which is produced by these servers. This Expensive infrastructure should be developed; operated and maintained very carefully as it produces greenhouse gases which are adverse to environmental balance. Proper cooling system and mechanisms are maintained by cloud centres to maintain the cloud infrastructure as environment friendly [25].

2.8 Able distributed computing with virtualization

In distributed and cloud computing environment, the concept of virtualization plays a very important role. This refers to the process of creating virtual machines for the various physical resources. This concept is closely related to task scheduling process where task queue is mapped to various virtual machines for scheduling. The main advantages of virtualization are cost reduction, highly scalable and provide elastic behaviour to the cloud computing environment [26].

2.9 Cost sensitive infrastructure with better throughput

According to cloud computing, bandwidth refers to the rate in which bits are transferred. This measurement is mainly useful when we are calculating throughput of the system. Since cloud computing environment is providing high speed transfer of data among systems it requires high bandwidth [27].

3 Machine Learning Based Cloud Models- Google Cloud Machine Learning Engine: A Case Study

Various machine learning algorithms which are used in cloud security and privacy are shown in fig. 1.

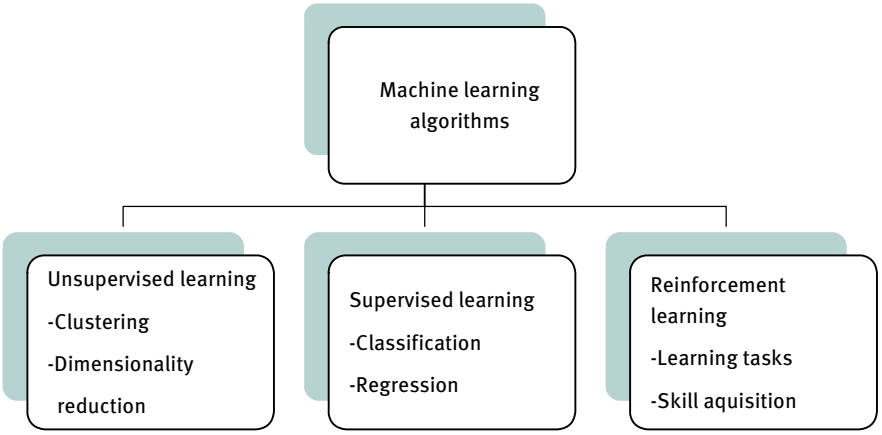

Fig. 1: Machine learning algorithms- Overview

In cloud computing and other environments, there are many similarities and differences in resource planning. The objective of scheduling is to achieve remarkable difference in resource usage. In traditional and conventional resource mapping scheduling, objects used are threads, jobs and tasks that pertain to the well-defined well- grained mapping and scheduling of entity resources. The cloud scheduling objects such as tasks and jobs are virtual machines (VM) belonging to the well-grained mapping and scheduling. Google cloud is machine learning models to observe revolutionary changes in cloud resource management.

3.1 Google cloud platform introduction

There are revolutionary changes arising in hardware and software that are equalizing machine learning (ML). Google Cloud Platform contains a separate kind of product or tools for various kinds of users such as beginners and specialists. For several years, Machine learning has been a supreme strength of Google's internal systems. Google cloud platform is providing proper frameworks, techniques, infrastructure, and information based on our requirement for data-driven systems on an outsized scale to satisfy customer's needs. Google is providing managed services that help

developers and scientists to make use of machine learning models. It is called Google Cloud Machine Learning (ML) Engine. Google Cloud Machine learning engines consists of advanced approaches and techniques [28]. There are many stages in machine learning workflow and they are illustrated as below.

- Collect all the sources and prepare the desired data
- Code your desired model
- Train, evaluate, assess and tune your model
- Deploy your designed trained model
- Obtain Predictions
- Monitor the systematic predictions
- Manage your designed model and its successive versions

Training of machine learning model on your data ensures training of the machine learning model, evaluating the accuracy of the model and tuning the hyper parameters of the model. Subsequent to training, deploying of your model takes place. Later than for prediction requests, model uses online or batch prediction [29-32]. Monitoring systematic or ongoing predictions is a continuous process to evaluate the performance of the machine learning model. The designed model has to be managed for its successive versions or deliveries.

Machine learning is a data analytics approach that trains computers to do as expected naturally similar to humans and natures: learn and get trained from the experience. Machine learning approaches use computational techniques to "learn" information directly from data without depend on a pre-programmed rules.

With the intensification in big data, machine learning has turn out to be a key method for solving difficulties in areas, such as:

- Computational finance
- Image processing
- Computer vision
- Computational biology
- Energy production
- Automotive
- Aerospace
- Manufacturing
- Predictive maintenance
- Natural language processing

Machine learning approach can be illustrated as shown in fig. 2.

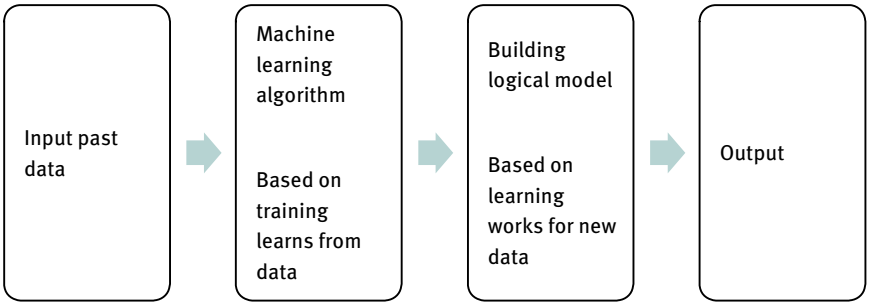

Fig. 2: Machine learning process- Outline

3.2 Various types of services

Various types of services are illustrated as shown in fig. 3.

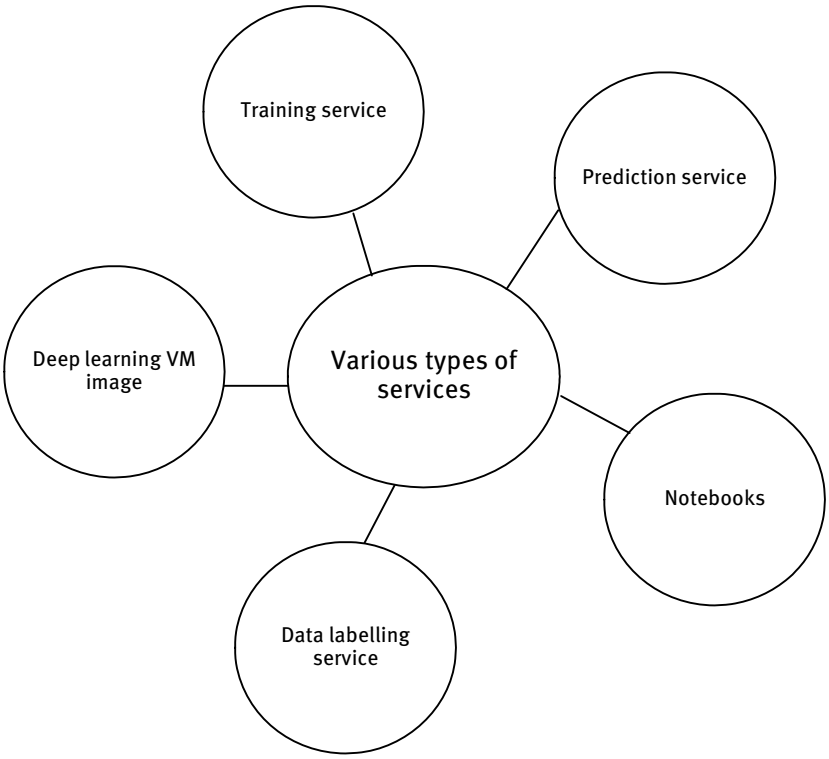

Fig. 3: Various types of services offered by machine learning algorithms

Machine learning algorithms identify natural patterns in the given data that create insight and aid you make improved decisions, forecasts and predictions. They are used every day to make critical decisions in medical analysis, stock trade-off, energy load prediction, and more.

3.2.1 Training service

Training service allows us to train the models and prototypes using a wide collection of different customization choices. Selection of different machine types allows us to power your training jobs, facilitate distributed training, practise using hyper parameter tuning, and accelerate with graphics processing unit or tensor processing unit.

3.2.2 Prediction service

Platform prediction service lets us to offer predictions based on a trained model, whether or not the model or prototype was trained on artificial intelligence platform.

3.2.3 Notebooks

Notebooks service allows us to create, manage and destroy virtual machine instances using virtual machine manager that are available in JupyterLab. These services contains pre-installed packages such as deep learning, TensorFlow and PyTorch. These instances are protected by google cloud authentication and they are easily integrate with GitHub repository.

3.2.4 Data labelling service

Data labelling service allows us to human labelling of dataset with text, image or video for training designed machine learning model. These services provides all the possible labels for the given dataset and instructions in what way these labels are given.

3.2.5 Deep learning VM image

Deep learning VM image allows us to choose from a set from set of images optimized for data science and ML tasks.

3.3 How to use google cloud machine learning?

Follow the below-mentioned steps to use Google Cloud Machine Learning

- Register to your Google account with your existing credentials
- Produce a Google Cloud Platform Project
- Change the Cloud Machine Learning Engine and cipher Engine arthropod genus
- Congratulations, you're exploiting Google Cloud Machine Learning Engine

3.4 Tools to interact with artificial intelligence platform

Follow the below-mentioned tools to interact with artificial intelligence platform.

3.4.1 Google cloud console

Using cloud console, we can manage and deploy loud models, versions and prototypes. This tool acts like an interface to work with AI resources by using tools such as cloud logging and cloud monitoring.

3.4.2 Gcloud command-line

Using Gcloud command line gcloud ai-platform, we can manage AI models, prototypes and versions to accomplish AI tasks at the command line. Gcloud commands and REST API are used for online predictions in AI platform.

3.4.3 REST API

REST API offers RESTful services for aiding online predictions.

3.5 Advantages of machine learning based google services

- Better productivity with fast access to invention and innovation: On a periodic basis Goggle AI system delivers updates in an efficient manner.
- Fewer disturbances when users adopt new features and functionality: Google gives new features and functionalities in a continuous stream.

- Global work culture in employees: Employees can access the services and information from anywhere in the world through web based applications of Google.
- Supports quick collaboration: Cloud users quickly access the data which is available in the cloud due to high availability of the services.
- Enhanced security with skilled personnel: Google has and hires skilled personnel to ensure next generation security in cloud.
- Ratio of data stored in cloud and local computers: Fewer data get stored in local devices to avoid vulnerability, whereas high amount of information and services are made available through cloud platform.
- High availability and reliability of the services: Due to redundant data centres, the data and services are made available to the cloud users with high availability and reliability.
- On demand scalable access and control to users: Through powerful Google apps users can have on demand scalable access and control over the services.
- Less expenditure and more gains: Google cloud based services allows users to access to them with less expenditure.

3.6 Statistical facts about machine learning

- International data corporation- IDC says that overall revenue in various industries including software, hardware and other service oriented is expected more than $156 billion in 2020. It has observed clearly with an increase of more than 12% over 2019.
- IDC's Worldwide Semiannual Artificial Intelligence Tracker says that global revenue will improve on by $300 billion by 2024, with CAGR (compound annual growth rate) of more than 17%.
- Forbes- Global media magazine says that AI based pricing and promotion have the potential to bring more than $259 billion in global market value.
- In telecom industry, explosion of data may increase the risk of security threats. Google cloud says that data traffic rate may cross 77 exabytes per month across the global market with a CAGR of 46% by 2022.
- Google says <0.1% of average Gmail mails is spam and in that 0.05% are useful mails. Spam mail prediction and detection is possible with machine learning algorithms.
- Intelligence through chatbots will reach $142 billion by 2024 from just $2.8 billion in 2019.
- Online education market may catch up to $350 billion by 2025 with machine learning technology.

4 Commercial Web Based Clouds based on Machine Learning

Cloud SIEM- Security information and event management system is shown in fig. 4.

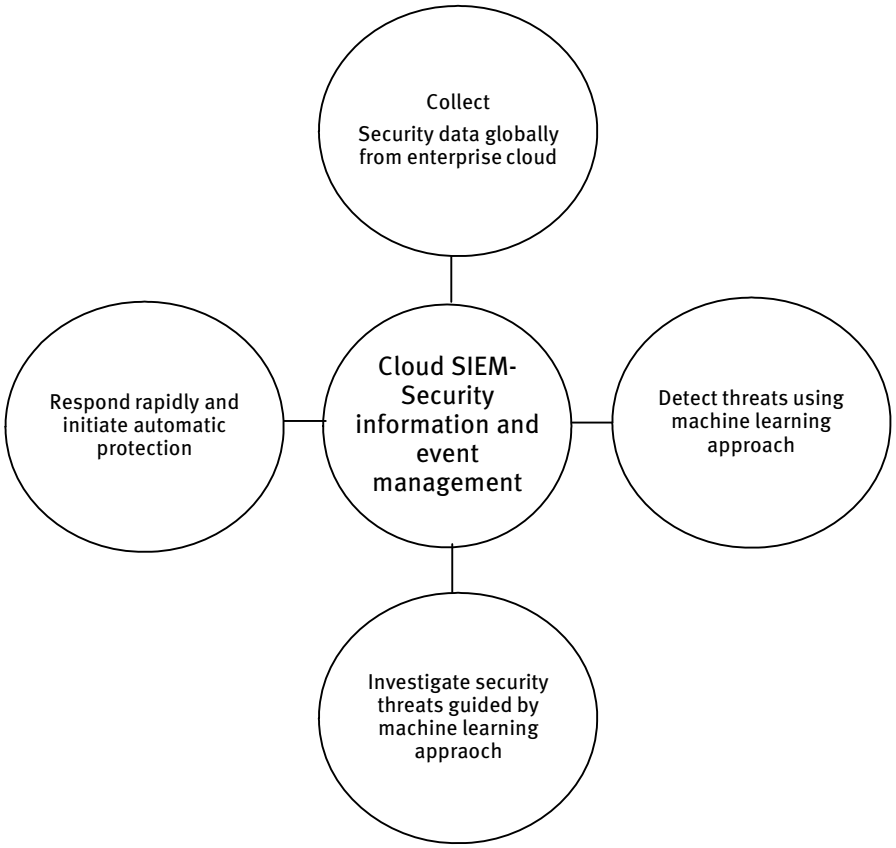

Fig. 4: Cloud SIEM- Security information and event management system

4.1 Cloud shell

Cloud shell is a web based environment which supports and manages resources by using online terminal with the aid of utilities, command line tools and libraries. Using cloud shell we can create cloud based applications. Google cloud shell includes cloud speech to text, app engine, data transfer and cloud build.

4.2 Various tools available in cloud shell

4.2.1 Persistent disk storage

Google cloud storage offers persistent disk storage using virtual machines and virtual machine manager interface on a pay per usage basis for every user. $HOME directory is mounted to provide this storage with various files such as home directory, software, scripts and configuration files.

4.2.2 Authorization

Google cloud API makes use of command line tools with authorization using Authorize Cloud Shell's dialog.

4.2.3 Pre-configured environment variables

When the cloud shell is initiated the project will be given to gcloud configuration system for immediate use. By using environment variable GOOGLE_CLOUD_PROJECT application default credentials of the library and active project also will be set in console.

4.2.4 Zone selection

Cloud shell is distributed in worldwide through various google cloud platforms. Initially it is assigned with the closest geographical region. Later, based on the workload it will try to migrate to other VMs.

4.2.5 Image rollout

Latest images of cloud shell gets updated with loud software development kit, Docker and required runtime utilities and libraries.

4.2.6 Root user

When you create user account you have all the privileges on the allocated virtual machine and you can execute workloads on it.

4.2.7 Available tools

These available tools are pre-installed and additional tools can be installed on a requirement basis. Additional tools which are installed on the virtual machine will not persist after instance gets terminated.

4.2.8 Language support

Various languages namely Java, Go, Python, Node.js, Ruby, PHP and .Net provides pre-installed language support.

4.2.9 Safe mode

Google cloud is using cloudshellsafemode=true in the URL to ensure safe mode and fix security issues in the files

4.3 Amazon Web Services

Amazon web services –AWS is a web based cloud platform launched in 2006 and provides various products such as Amazon sage maker, Amazon augmented AI, Amazon forecast, Amazon translate, Amazon personalize, AWS deep learning AMI's and Amazon polly.

4.3.1 Microsoft Azure

Microsoft azure is a web based cloud computing platform launched in 2010 and provides various products such as Microsoft azure cognitive service, Microsoft azure data bricks, Microsoft azure bot service, Microsoft azure cognitive search and Microsoft azure machine learning.

4.4 IBM Cloud

IBM cloud is a cloud computing platform provides several types cloud services such as public, private and hybrid with various products namely IBM Watson studio, IBM Watson speech-to-text, IBM Watson text-to-speech, IBM Watson natural language understanding, IBM Watson visual recognition and IBM Watson assistant.

5 State of the art Machine learning algorithms for cloud security

Various state of the machine learning algorithms are listed in the table 1.

Tab. 1: 6.State of the art machine learning algorithms

Algorithm	Machine learning algorithm	Remarks
A Review of Machine Learning Algorithms for Cloud Computing Security	Supervised, unsupervised, semi supervised and reinforcement	Security threats, issues, and associated solutions of cloud computing are stated
Assessment of machine learning algorithms in cloud computing frameworks	Supervised	Powerful analytical methods that allow machines to recognize patterns and facilitate human learning are stated
Network based IDS for cloud environment using combination of machine learning algorithms	Deep Neural Network (DNN) based anomaly Network IDS using a hybrid optimization framework (IGASAA) based on Improved Genetic Algorithm (IGA) and Simulated Annealing Algorithm (SAA)	Reduced execution time, convergence time and save processing power
Feasibility of Supervised Machine Learning for Cloud Security	Supervised	Demonstrates the effectiveness of these models across multiple datasets by improving cloud security
Evaluating machine learning algorithms for anomaly detection in clouds	Supervised and unsupervised	Detects abnormal behaviour of services and hosts by analysing metrics collected from all layers and components of the cloud infrastructure

Code for machine learning algorithms such as linear regression, support vector machine and Naive Bayes classification is given as below.

Listing 1: Code for machine learning algorithms such as linear regression, support vector machine and Naive Bayes classification

```
#Linear regression
lin_regr = linear_model.LinearRegression()
lin_regr.fit(X_train, y_train)
print(lin_regr.coef_)
```

```
print(lin_regr.score(X_test, y_test))
plt.style.use('fivethirtyeight')
plt.scatter(lin_regr.predict(X_train), lin_regr.predict(X_train) -
y_train, color = "yellow", s = 10, label = 'Training data')
plt.scatter(lin_regr.predict(X_test), lin_regr.predict(X_test) - y_test,
color = "pink", s = 10, label = 'Testing data')
plt.hlines(y = 0, xmin = 0, xmax = 100, linewidth = 5)
plt.legend(loc = 'upper right')
plt.title("Demo")
plt.show()
#Support vector machine
from sklearn import svm as s
from sklearn import metrics as m
s_class = s.SVC(kernel='linear')
s_class.fit(X_train, y_train)
y_pred = s_class.predict(X_test)
print(m.accuracy_score(y_test, y_pred))
print(m.precision_score(y_test, y_pred))
print(m.recall_score(y_test, y_pred))
#Naive Bayes Classification
import numpy as n
import pandas as p
from sklearn.naive_bayes import GaussianNB
from sklearn.metrics import confusion_matrix, accuracy_score
NB_class = GaussianNB()
NB_class.fit(X_train, y_train)
y_pred = NB_class.predict(X_test)
ac_sc = accuracy_score(y_test,y_pred)
cm_ma = confusion_matrix(y_test, y_pred)
```

6 Conclusion

Machine learning has currently become a part of our daily lives, and is a new technology endowed, to handle security and privacy problems that arise in cloud computing. In recent years, in depth analysis was administered on the protection and privacy problems of cloud computing. Therefore, security and privacy become terribly essential and vital and are to be addressed. For future work, it's essential for the researchers to deeply investigate different science primitive's solutions for security attacks in cloud computing. A mixed protocol technique will scale back the computation overhead on the protection and privacy protective solutions. Moreover, cus-

tomization of the privacy and security protocols for machine learning is additionally a noteworthy and open analysis space to develop a viable resolution. Research is looking forward to perform their analysis within various applications of machine learning such as space of astronomy, natural philosophy, nucleonics, physical science, magnetism, machines, technology, mechanics, electro hydrokinetics, signal process, power, energy, bioinformatics, economy, and finance.

7 References

[1] Dillon T, Wu C, Chang E, Cloud Computing: issues and challenges, 2010 24th IEEE International Conference on Advanced Information Networking and Applications, Perth, WA, Australia, 2010, pp. 27-33, doi: 10.1109/AINA.2010.187

[2] Wang L, Laszewski V, Younge A, Cloud Computing: a perspective study, New Gener. Comput, 2010, 28, 137–146, https://doi.org/10.1007/s00354-008-0081-5

[3] Naveen G, Ayushi G, Survey on machine learning based scheduling in cloud computing, Proceedings of the 2017 International Conference on Intelligent Systems, Metaheuristics & Swarm Intelligence, Association for Computing Machinery, New York, NY, USA, 2017, 57–61, DOI:https://doi.org/10.1145/3059336.3059352

[4] Umer A, Muhammad M, Shah S, Amin R, Shaukat W, Syed R, Suh Y, Piran J, A review of machine learning algorithms for cloud computing security, Electronics, 9, 2020, no. 9: 1379, https://doi.org/10.3390/electronics9091379

[5] Subramanian K, Tamilselvan L, A focus on future cloud: machine learning-based cloud security, SOCA, 2019, 13, 237–249, https://doi.org/10.1007/s11761-019-00270-0

[6] Bhamare D, Salman T, Samaka M, Erbad A, Jain R, Feasibility of supervised machine learning for cloud security, 2016 International Conference on Information Science and Security (ICISS), Pattaya, Thailand, 2016, pp. 1-5, doi: 10.1109/ICISSEC.2016.7885853

[7] Nassif A, Talib M, Nasir Q, Albadani H, Dakalbab F, Machine learning for cloud security: a systematic review, IEEE Access, 2021, vol. 9, pp. 20717-20735, doi: 10.1109/ACCESS.2021.3054129

[8] Han Q, Meikang Q, Zhihui L, Selective encryption on ECG data in body sensor network based on supervised machine learning, Information Fusion, 2020, Volume 55, Pages 59-67, ISSN 1566-2535, https://doi.org/10.1016/j.inffus.2019.07.012

[9] Potluri S, Mangla M, Satpathy S, Mohanty S N, Detection and prevention mechanisms for DDoS attack in cloud computing environment, 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2020, pp. 1-6, doi: 10.1109/ICCCNT49239.2020.9225396

[10] Karimipour H, Dehghantanha A, Parizi R, Choo K, Leung H, A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids, IEEE Access, 2019, vol. 7, pp. 80778-80788, doi: 10.1109/ACCESS.2019.2920326

[11] Wu W, Alvarez J, Liu C, et al., Bot detection using unsupervised machine learning, MicrosystTechnol, 2018, 24, 209–217, https://doi.org/10.1007/s00542-016-3237-0

[12] Çavuşoğlu Ü, A new hybrid approach for intrusion detection using machine learning methods, ApplIntell, 2019, 49, 2735–2761, https://doi.org/10.1007/s10489-018-01408-x

[13] Potluri S, Achyuth S, Elham T, Mohanty S N, IOT enabled cloud based healthcare system using fog computing: a case study, Journal of Critical Reviews ISSN- 2394-5125, 2020, Vol 7, Issue 6, PP: 1068-1072, doi: 10.31838/jcr.07.06.186

[14] Mahmud R, Fernando K, Rajkumar B, Cloud-fog interoperability in IoT-enabled healthcare solutions, ICDCN '18: Proceedings of the 19th International Conference on Distributed Computing and Networking, 2018, Article No.: 32 Pages 1–10, https://doi.org/10.1145/3154273.3154347
[15] Subramanian E, Tamilselvan L, A focus on future cloud: machine learning-based cloud security, Service Oriented Computing and Applications, 2019, 13, 10, 10.1007/s11761-019-00270-0
[16] marwan m, kartit a, ouahmane h, security enhancement in Healthcare Cloud using Machine Learning, Procedia Computer Science, 2018, Volume 127, Pages 388-397, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2018.01.136
[17] Sen J, Security and privacy issues in cloud computing, ArXiv, abs/1303.4814, Khanghahi N, Ravanmehr Reza, Cloud Computing Performance Evaluation: Issues and Challenges, International Journal on Cloud Computing: Services and Architecture (IJCCSA) ,2013, Vol.3, No.5, 3. 10.5121/ijccsa.2013.3503
[18] Sinha N, Khreisat L, Cloud computing security, data, and performance issues, 2014 23rd Wireless and Optical Communication Conference (WOCC), 2014, Newark, NJ, USA, 2014, pp. 1-6,doi: 10.1109/WOCC.2014.6839924
[19] Lehrig S, Eikerling H, Becker S, Scalability, elasticity, and efficiency in cloud computing: a systematic literature review of definitions and metrics, 10.1145/2737182.2737185, Rashidi B, Sharifi M, Jafari T, A Survey on Interoperability in the Cloud Computing Environments, I.J.Modern Education and Computer Science, 2013, 6, 17-23, 10.5815/ijmecs.2013.06.03
[20] Potluri S, Subbarao K, Improved quality of service-based cloud service ranking and recommendation model, TELKOMNIKA Telecommunication, Computing, Electronics and Control, 2020, Vol. 18, No. 3, pp. 1252~1258 ISSN: 1693-6930, DOI: 10.12928/TELKOMNIKA.v18i3.11915
[21] Potluri S, Subbarao K, A hybrid PSO based task selection and recommended system for cloud data, Test Engineering and Management, 2020, Vol-83, ISSN: 0193-4120 PP: 10210 – 10217
[22] Potluri S, Subbarao K, Hybrid self-adaptive PSO and QoS based machine learning model for cloud service data, International Journal of Control and Automation, 2020, Vol. 13, No. 2s, pp. 36 - 50, ISSN: 2005- 4297
[23] Nguyen T, Berder O, Sentieys O, Energy-efficient cooperative techniques for infrastructure-to-vehicle communications, IEEE Transactions on Intelligent Transportation Systems, 2011, vol. 12, no. 3, pp. 659-668, doi: 10.1109/TITS.2011.2118754
[24] Potluri S, Varshith K, Software virtualization using containers in google cloud platform, International Journal of Innovative Technology and Exploring Engineering (IJITEE), 2019, ISSN: 2278-3075, Volume-8 Issue-7
[25] Nguyen T, Berder O, Sentieys O, Energy-efficient cooperative techniques for infrastructure-to-vehicle communications, IEEE Transactions on Intelligent Transportation Systems, 2011, vol. 12, no. 3, pp. 659-668, doi: 10.1109/TITS.2011.2118754
[26] Challita S, Zalila F, Gourdin C, Merle P, A precise model for google cloud platform, 2018 IEEE International Conference on Cloud Engineering (IC2E), 2018, Orlando, FL, USA, pp. 177-183, doi: 10.1109/IC2E.2018.00041
[27] Shabani I, Kovaçi A, Dika A, The benefits of using google cloud computing for developing distributed applications, Journal of Mathematics and System Science, 2015, 5, 156-164, doi: 10.17265/2159-5291/2015.04.004
[28] Butt A, Mehmood M, Shah H, Amin R, Shaukat W, Raza M, Suh Y, Piran M, A review of machine learning algorithms for cloud computing security, Electronics, 2020, *9*, 1379, https://doi.org/10.3390/electronics9091379
[29] Li K, et al., Assessment of machine learning algorithms in cloud computing frameworks, 2013 IEEE Systems and Information Engineering Design Symposium, Charlottesville, VA, USA, 2013, pp. 98-103, doi: 10.1109/SIEDS.2013.6549501

[30] Chiba Z, Abghour N, Moussaid K, Amina E, Mohamed R, Intelligent approach to build a deep neural network based IDS for cloud environment using combination of machine learning algorithms, Computers & Security, 2019, Volume 86, Pages 291-317, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2019.06.013

[31] Bhamare D, Salman T, Samaka M, Erbad A, Jain R, Feasibility of supervised machine learning for cloud security, 2016 International Conference on Information Science and Security (ICISS), Pattaya, Thailand, 2016, pp. 1-5, doi: 10.1109/ICISSEC.2016.7885853

[32] Gulenko A, Wallschläger M, Schmidt F, Kao O, Liu F, Evaluating machine learning algorithms for anomaly detection in clouds, 2016 IEEE International Conference on Big Data (Big Data), Washington, DC, USA, 2016, pp. 2716-2721, doi: 10.1109/BigData.2016.7840917

Sirisha Potluri, Gouse B. Mohammad, Sachi Nandan Mohanty, M. Vaishnavi, K. Sahaja

Secure Intelligent Framework for VANET: Cloud Based Transportation Model

Abstract: Vehicular cloud computing has a prodigious impact on information technology solutions. According to VCC the unexploited computing resources are parking vehicles, vehicles stuck in congestion, parked cars in any place. VCC architecture has three layers. Some of the developments that are taking place in the automobile industry for the last few decades have been very interesting and resolution driven. A lot of safety applications, convenience and commercial applications are proposed for the VANET's by researchers and by the US department of transportation. The vehicles connect together through a network to form a vehicular cloud which will offer space for storing, computing resources, sensor readings as an on-demand service to clients. Traffic is becoming a daily and even growing phenomenon which spoils the valuable time, fitness and energy of human. There is a need of efficient computational, supervising and guiding solutions for the citizens to make them to get rid of traffic related issues and problems. Finding an appropriate parking lot within the area on the brink of university, shopping complex, or a commercial complex in big and medium cities would enjoy the assistance of an automatic parking management utility.

Keywords: Vehicular Cloud Computing, Intelligent Transportation Systems, Cloud Security, Cloud Privacy, Vehicular Ad Hoc Network, Internet of Things

Sirisha Potluri, Department of CSE, IcfaiTech (Faculty of Science and Technology), ICFAI Foundation for Higher Education, Donthanapally, Shankarpalli Road, Hyderabad, Telangana 501203, India, sirisha.vegunta@gmail.com
Gouse Baig Mohammad, Department of CSE, Vardhaman College of Engineering, Hyderabad, Telangana 501218, India, gousebaig@vardhaman.org
Sachi Nandan Mohanty, Department of Computer Engineering, College of Engineering Pune, Wellesley Rd, Shivajinagar, Pune, Maharashtra 411005, India, sachinandan09@gmail.com
M. Vaishnavi, Department of CSE, IcfaiTech (Faculty of Science and Technology), ICFAI Foundation for Higher Education, Donthanapally, Shankarapalli Road, Hyderabad, Telangana 501203, India, sudhakar.maheshuni@gmail.com
K. Sahaja, Department of CSE, IcfaiTech (Faculty of Science and Technology), ICFAI Foundation for Higher Education, Donthanapally, Shankarapalli Road, Hyderabad, Telangana 501203, India, sahajakamtam408@gmail.com

https://doi.org/10.1515/9783110732573-008

1 Introduction to VANET

Some of the developments that are taking place in the automobile industry for the last few decades have been very interesting. Vehicles today are considerably more fuel-efficient than they were before. Even in today's time the vehicles are prone to accidents due to mist, smoke, dust and various other death-traps on the road but above all of that they are much more vulnerable to accidents that are taking place due to human errors.

However much of these fatal human errors are about to reduce because the automobile industry can been working vigorously for many year to put different kinds of sensors in the cars and connect them to an on-board computer system. With the development in the technology telecommunications and broadcastings has now become potential to connect vehicles to each other through wireless technologies to enable them to interconnect and work together. Autonomous vehicles are being supported by the governments in this present age.

A lot of funding is provided for research on driver-less cars from various governments especially from UK. This funding is bringing about the merging of various companies together which not only include the companies from automobile sector but also from information technology, telecommunications to work together.

Many car manufacturers such as Ford, Hyundai, and Tata etc. have released application development for their platforms by making their application program interface- API available to other developers. The developers submit their apps and approve them before making them available for download. The long term evolution-LTE connectivity ensues to serve and improve the in-vehicle presentation services by providing entrance and access to high-speed internet, streaming movies, navigation control, music applications, and live television and so on. The other feature is commercial and profitable which offers location-based services and ads to the vehicle travellers. The LTE connectivity helps in bringing the internet not only to the vehicle but also makes the vehicle a part of the internet paving the way for the vehicular ad hoc networks (VANETs).

The true future prospective of the connected vehicle can only be realized when vehicles are interconnected to each other. This network that is formed by the interconnection of vehicles is referred to as VANET. This shift in vehicular technology will bring about a new era of innovation and will open a huge range of application areas that can help in improving road safety and reducing accidents on roads.

VANETs are considered to be significant because of their huge potential and several applications that are being made accessible. VANETs not only offer strong safety enhancements but also provide a lot of commercial openings and opportunities. Wireless access in the vehicular environment (WAVE) delivers the basic radio standard for dedicated short range communication (DSRC) in VANETs.

Vehicles use DSRC radios to connect and communicate with each other in two ways namely vehicle-to-vehicle communication (V2V) and vehicle-to-infrastructure communication (V2I). The communication range of dedicated short range communication lies in the range between 300 to 1000 m. With the addition of 4G/LTE connectivity in vehicles it has become obvious that connected and networked vehicles have the facility to share data by means of the cloud. The gains of using cloud in connected vehicles are enormous as the opportunities for using applications are virtually limitless.

DSRC identifies one main type of message which is called as the basic safety message (BSM) that a vehicle communicates and transmits every 100 milli seconds. In basic safety message the vehicles broadcast the details of their location, speed, acceleration, and several other useful parameters which can help other vehicles in avoiding collisions and generate warnings for having improved safety measures. These messages also help the vehicles and auto mobiles in maintaining the list of their neighbours.

The navigation systems has been made available but the exact real-time location information of other vehicles is not yet available. This is an area in the future that can enable the driver to drive safely on roads even if there is nil visibility or when the driver is not capable to drive the vehicle. Therefore, the vision is to generate a mutual understanding among all vehicles on the road that can lead to driverless cars.

All the vehicles can be programmed and automated by using software to transmit and share their location and other related important information whenever they observe an unexpected change in speed or position while driving. However, the bandwidth in DSRC is quite limited, so when the vehicles try to transmit their location or position and speed information there is a possibility of having a jammed channel. The DSRC and 4G/LTE connectivity in vehicles can support each other and answer the bandwidth problem to give great quality, consistent, reliable, and secure information to VANET users [1-5].

2 Constraints of Cloud

Cloud computing offers on demand services to the customers using efficient resource usage and allocation based policies and protocols by matching with the service level agreement. Service level agreement commonly includes various segments like measuring the performance, managing the problems, customer satisfaction, recovery from failures and finally termination of the agreement. SLA's are consistently checked and validated using which it creates a better communication channel between consumer and the provider. SLA establishes the Quality of Service (QoS) agreement between service-based system providers and users. With a violation of

SLA, the provider must pay penalties. Continuous performance check is required in order to ensure that these CSPs are providing services as mentioned in SLAs. SLA is consistently met, these agreements are frequently designed with specific lines of demarcation and the parties involved are required to meet regularly to create an open forum for communication. Cloud computing is using collection of resources and all these are supported by the interface and infrastructure concept of distributed and cloud computing environment. Service level agreement can be viewed as a document between customer and provider and is mainly based on services and not on customers [6-10].

3 Applications of VANET

A lot of safety applications, convenience, business and commercial applications are proposed for the VANET's by researchers and by the US department of transportation. Some of these applications are discussed briefly below. With numerous vehicles on the roads having such as lot of computing power and sensors, it's apparent and logical to utilize all this data to make a highly mobile unplanned networks [11]. Some of the applications that are recommended for VANETs are as follows.

3.1 Safety applications

Some of the safety applications include:

- Sending notifications if any crashes occur.
- Threats that might happen on the roads due to bad, slippery or wet road conditions in cases of heavy rains.
- Traffic breaking warnings and curve speed warnings in case of fast speed or negligence.
- Emergency electronics traffic control or any pre-crash feel and co-operative forward collision warnings.

Some of the safety precautions might also include warning messages that are given to drivers in order to inform them about approach of any emergency vehicles.

3.2 Convenience applications

Some of the convenience applications include:

- Navigation and personal routing is provided to reach destination, stoppage advice is given in case of heavy traffic.

- Toll group and parking availability information is provided for convenience of drivers.
- Road and weather are often monitored by sharing the information from on-board vehicle sensors.
- The vehicular network can turn into the crisis and emergency transmission device.

The connected and networked vehicles can play a really important role in situations such as power disruption and network breakdown as they need on-board batteries and lots of sensors including cameras which provide valuable images and SOS calls.

3.3 Commercial applications

Some of the commercial applications include:

- Location-based facilities and services like advertisements, announcements and entertainment which include data/information/video relay, social networking informs.
- By using vehicle to vehicle communication and vehicle to infrastructure communication information such as vehicle positions and information on road conditions can be easily communicated.

Furthermore, the driving force may have to form life-saving decisions that are supported by the knowledge received such as hand brake light, onward collision warning. It is therefore extremely important that the privacy, security, reliability, and integrity of the messages are ensured and safeguarded in order that actions are taken immediately after the knowledge is received.

4 VANET- Cloud Based Approach

The great amount of unused and idle space for storing and computing power including on-board sensors provide a singular opportunity to use vehicles as a wireless sensor network. The vehicles are going to be equipped and furnished with not only sensors to live temperature, rainfall, humidity, wind, etc., but also with cameras. This alongside high speed (4G/LTE) connectivity are often an excellent benefit for a spread of cloud based vehicle applications [12].

4.1 VANETs within the cloud

The connected and networked vehicles can link with the cloud and can upload their data which include sensor readings and traffic information that can be downloaded by other vehicles that are following behind schedule. This enables the users to share data unknown and preserve security and privacy of information that is being provided as shown in fig. 1. The application servers that are embedded within the cloud can collect and add the knowledge coming in from vehicles and then bring together that information to form announcements and declarations for traffic, road conditions and surroundings, accidents and weather supported vehicle sensor data. This progresses the reliability of the knowledge by filtering out the biased or dishonest information gauged by the amount of users or consumers reporting such information.

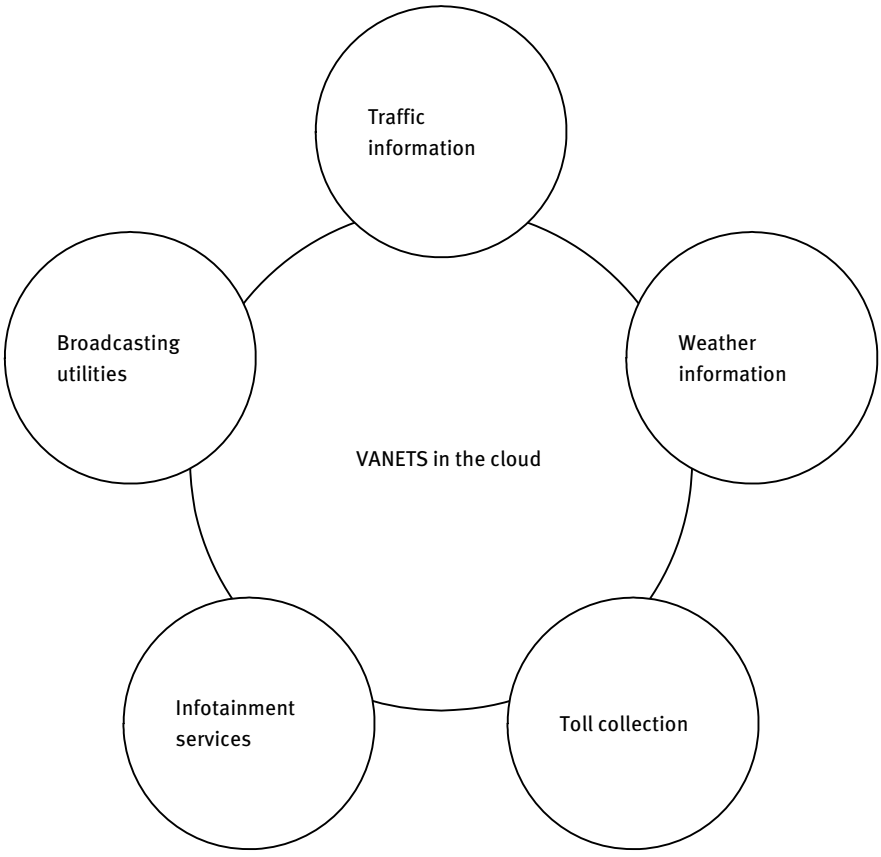

Fig. 1: VANETs in the cloud

4.2 Vehicular cloud

The vehicles join and connect together through a network to form a vehicular cloud which will offer space for storing, computing resources, sensor readings and interpretations as an on-demand service to clients. The clients who demand such services may be individuals, organizations, corporations and government departments like the meteorology, climatology department, police department or highway authorities as shown in fig. 2. Moreover, with cameras on board vehicles and high-speed connectivity, the police or disaster services can even appeal images from vehicles for a neighbourhood that they need to watch like the location of an accident [13].

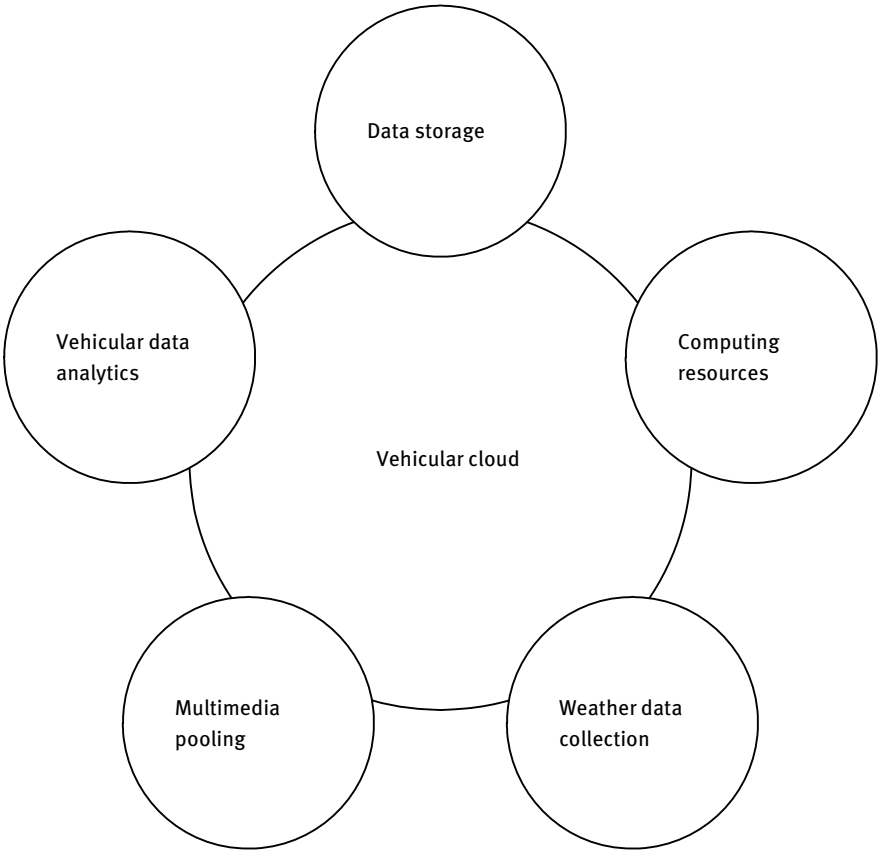

Fig. 2: Vehicular cloud

4.3 Private vehicular cloud

The computing resources, storage facilities of the vehicle are often used by the owner as a personal cloud in which the user attaches to the web and uploads all of the data into a private cloud as shown in fig. 3. By storing all of the data into a private cloud one can get ownership of data and view it whenever it is required [14].

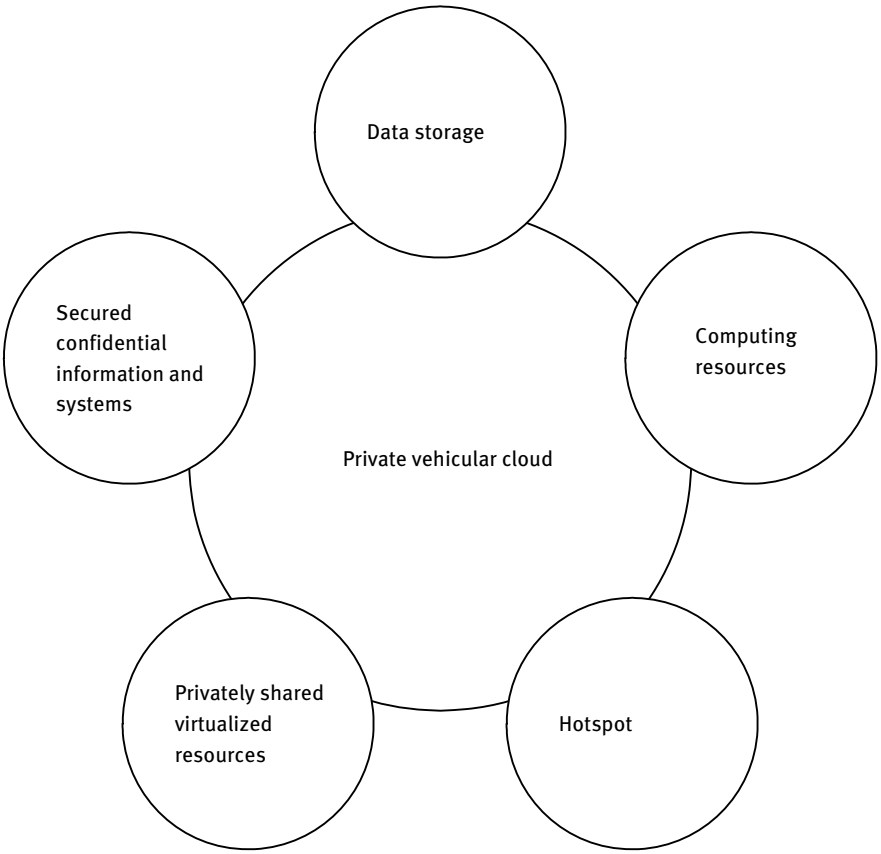

Fig. 3: Private vehicular cloud

5 Autonomous/Self-Governing Vehicle

The autonomous or self-governing vehicle may be a certainty today through Google car and it's only logical to mention that the technology and expertise will improve further and decrease in cost to become a feature within the near future. However,

it'll take a while for it to develop a driver-less feature on a massive scale. Also, it's possible that very similar to control, this might become a feature that would be simulated and activated on the motorway or highway. Autonomous vehicles would wish almost no input from the driving force. This is able to be possible with tons of hardware like sensors, cameras, radars, locators and laser illuminated detection and ranging (LIDAR) to sense approaching obstacles and hurdles. Image processing practices are applied to pictures from the cameras to acknowledge, classify and identify the various shapes and features. This permits the vehicle to sense the upcoming hurdle or obstacle and spontaneously apply breaks or reduce speed far more rapidly than the driving force would ever be ready to. The utilization of those and other technologies therefore safeguards that human errors are often abridged to an outsized extent and, as an outcome, roads are regularly made much safer. This is able to enable the driving force to be more dynamic by doing something like reading, evaluating and browsing on the web or making a call.

Autonomous vehicles aren't only an opportunity but an essential for safe motoring. Subsequent step in autonomous or self-governing vehicles is vehicle swarm [15].

6 Vehicle Platoon/Swarm

Travelling at great speeds take along more problems however, these problems are often abridged if the vehicles form a gaggle then travel during the creation on highways and motorways. This may have two benefits:

- Vehicles are synchronized and corresponded (i.e., vehicles travel during a line and maintain a hard and fast distance from one another and therefore the vehicle ahead informs the cars behind if they ought to reduce speed or change lanes beforehand , then all of them can roll in the hay in tandem)
- The randomness within the immediate neighbourhood of the vehicles is reduced, which makes things much simpler and harmless.

Safe road trains for the environment (SARTRE) is an EU-endow more than 6 million dollar project that has exhibit this idea together with Volvo, Ricardo and among others. The purpose of the SARTRE development was to develop a road train or platoon conception in vehicle traffic where a lead vehicle driven by well-informed driver takes control of a platoon of vehicles that enter a semi-independent state. The SARTRE project established successfully that vehicle platoons aren't only safe but are often very efficient in reducing congestion and improving safety. The vehicle swarm are often imaginary by thinking of the motorway/highway as a conveyer belt, but where a conveyer belt moves with a continuing steady speed, a gaggle of vehicles on the auto route can move with any set sustained speed. This will be probable by agreeing like-minded vehicles, i.e., vehicles that shall travel at roughly an equiv-

alent speed, to team and form groups or a “vehicle swarm”. Ricardo, a British engineering firm convoluted within the SARTRE project, considers that vehicle platooning is feasible with fully autonomous or self-governing vehicles [16].

7 Applications of Vehicular Cloud Computing

7.1 Parking lot data or information based cloud

Topical US-DOT indicators reveal that the registered vehicular convoy on American streets and roadways is nearly 256 million vehicles are strong and rising gradually. Also, statistics disclose that most of those vehicles spend numerous hours per day parked for the duration of a parking garage, parking region, or driveway. Allow us to consider a small company paying a couple of hundred people and given that IT services. We leave carpooling and vehicles remain parked in the parking lot. In those vehicles, the algorithmic resources have no use and persist inactive for hours. The corporate can give an intention for the employees who will rent the resources for the VC formation. Hence, the contributing and take part vehicles within the parking lot create a computer vehicle cluster and supply ample services for secured data storage [17].

7.2 Dynamic and self-motivated traffic light management

Todays, thanks to amassed variety of vehicles on the roads, the traffic is flattering a daily phenomenon which wastes the valuable time, resources, energy and fitness of the human. One among the finest solutions to worn out this issue is to allocate the appropriate quantity of resources instead of pre-allocating of massive resources as a basis for the worst condition. Allow us to think through an occasion like a football match that’s appeared by thousands of individuals, where a traffic congestion may occur at the top of the diversion. Even though range of studies and trainings are accomplished to deal with this subject by leveraging VANETs and IT’S, they are unable to testimony traffic problems rapidly and typically cannot provide a traffic alleviation plan. VCC is in a position to present an additional well-organized and cost-effective thanks to solve the traffic jam by providing the definite resources from the available vehicles contributing within the traffic and connecting them in finding a solution unconventionally without expecting officials react [18].

7.3 Optimizing and enhancing traffic signals

Traffic signals set the sign cycle length and consequently the green phase lengths. Signal system optimization is presently take place off line at either out of the way connection or the passageway level. The time periods are well-defined by the timing strategies surely time periods, such as the workaday morning or afternoon greatest peak hours. One among the drawbacks of this method is that it requires data on traffic whirling movements that are frequently collected to make guaranteed that the signal timing strategies are appropriate for the present traffic capacity conditions. Another difficulty is that this plan does not cope well with indefinite changes in traffic circumstances and environments. Thus, scan exploits the signal system enactment by making active use of a vehicular network.

7.4 Road safety communication and message

New cars have embed detecting devices for skilful and safe operation. The cameras help the driving force by chasing the lines on the road and support them in staying within the path. Thus, cars have a sensor node, and a VC can form dynamic with a big wireless sensor network. Vehicles review the sensors of other cars in close nearness to extend the loyalty and obtain a valuation of the probable road risk ahead, the road conditions, speed breakers, dumps, and snow. However, this VANET design will not give us the direction of safety measures and a quicker solution.

7.5 VC in developing countries

Due to lack of skilled centralized decision support systems and provision, the idea of VC are going to be very significant in emerging countries also. Moreover, VCs will play a significant role in making a vast number of computing resources reachable through a vehicular network by using many computing applications dynamically, which aren't likely to use with the existing infrastructure.

7.6 Managing parking facilities

Finding an appropriate parking lot within the area on the brink of university, shopping complex or in big cities would enjoy the assistance of an automatic parking controlling utility. Recently, the recognised solutions reinforced a unified style from single parking garages and parking meters have been joined then spread to the community. Today, the vehicle drivers are capable to find a parking lot by means of their smartphone applications (e.g., Smart park, Park Me and Park Mate). However, these applications have some disadvantages that haven't been addressed, such as:

covering the incomplete point of the planet and therefore the need for accessing internet. The vehicles that form the VC during a specific area will accomplish real time data of accessible parking spaces and initiate drivers to the most appropriate position [19].

8 Characteristics of VANET

The characteristics of VANETs consist of high mobility and regular change in topology. Some of the characteristics of VANETs are discussed below:

8.1 High mobility

VANETs have great mobility. Having high mobility in VANETs essentially helps in playing a very significant role in the demonstrating of VANET protocol. Every node that exist in a VANET moves on very great speed which allows the great mobility of nodes and decreases the communication time in the vehicular network.

8.2 Driver safety

VANETs can support in educating the driver safety, improve the passenger ease level and progress the traffic flow. One of the foremost gain of VANETs is that the vehicles can connect and communicate directly with each other. It allows a number of submissions to connect and communicate among different nodes such as the Road side units (RSU) and On-board units (OBU).

8.3 Dynamic network topology

The topology of VANETs can change quickly based upon the vehicle speed and great mobility. The changes that are taking place in the flexibility of the vehicles are creating the VANETs more horizontal to various kinds of attacks and it is also becoming a very hard job to distinct the suspected vehicles.

8.4 Frequent network disconnection

The regular suspension and disconnection of the VANETs are become high-speed measure among vehicles and various other usual conditions such as weather. A

large amount of vehicles on the road can also lead to the regular disconnection in the service.

8.5 No power constraints

There is certainly no power constraint in VANETs .This allows the vehicle to deliver constant power to the on-board units by the means of a long-lasting battery.

8.6 Network strength

The network strength of VANETs be influenced by the flow of the traffic on the roads. If there is a case of traffic congestion the network strength can be very high and if there is completely no traffic it can be low. The network can be superior nearby highways and close to the entry and exit locations of the city.

8.7 Large computational processing

The nodes that are existing in the VANETs are vehicles which can be inserted with the sensors and some of the other computational devices such as processors, antenna and GPS. All of these resources will need to have a great quantity of computational capacity of the node in the VANET and provide healthier wireless communication to obtain specific information relating to position, speed and direction.

9 Security Services of VANET

The security and safety of the VANETs is an important issue for providing safety to the person along for the ride and drivers. The security services are as follows:

- Availability of the service
- Confidentiality of the service
- Authentication of the service
- Data integrity of the service
- Nonrepudiation of the service

9.1 Availability of the service

The feature of Availability plays an extremely crucial role in the security of the VANET because it will ensure that the network will always remain functional in a lot

of faulty and unpredicted conditions. This feature of availability has become extremely prone to some of the dangerous attacks as compared to some of the other security services that are available. Hence a lot of trust-based and cryptography practices can be used to secure the VANETs from these outbreaks.

9.2 Confidentiality of the service

Confidentiality guarantees that the data and records can be accessed only by the dedicated user while it makes impossible for unauthorized users to access the private and confidential information that communicates to the designated user.

9.3 Authentication of the service

The authentication shows an important role to guarantee the safety of the VANET. It prevents the vehicles from malicious activities that might take place in network. In order to avoid the network from dangerous outbreaks it is necessary that the authentication of users and messages which permit through the network is required.

9.4 Data Integrity of the service

The feature of Data integrity helps to ensure that the content of the message is not changed or altered in any sense during the process of transmission.

9.5 Nonrepudiation of the service

The feature of nonrepudiation is very important as it ensures the validity and makes sure that the sending and receiving entities cannot reject its transmission and reception in case of any disagreement.

10 Threats and Attacks of VANETs

The VANETs go through different types of threats and attacks and the destruction caused by these attacks can cause distress to various other applications. The adverse impact of some of the attacks effects many processes and measures. Some of these applications include safety, security, comfort, and infotainment.

10.1 Attack on communication

In VANETs it is difficult to achieve secure communication because the VANETs security goes through many threats such as certificate duplication attack, eavesdrop attack, and location confidentiality or privacy attack.

10.1.1 Certificate replication attack

In this type of attack attacker may use false certificates and keys of the other users as an evidence of authentication without getting tracked. The main purpose of such a type of attack is to create confusion and make it harder to identify the malicious vehicle.

10.1.2 Eavesdrop attack

This type of attack finds the confidential and personal information when a non-registered vehicle uses a valid and legal certificate to collect all of the valuable information of the vehicles such as user ID, vehicle location etc.

10.1.3 Privacy attack

This type of attack includes different kinds of outbreaks on privacy-preserving schemes that can include something like tracking of a vehicle. For suppose the attacker might try to use the location of the target vehicle, ID, significant and credential to initiate alternative attack without getting tracked.

10.2 Attack on safety applications

These attacks are associated and related to the channel allocation

10.2.1 Denial of service attacks

This is one of the most common outbreaks in VANETs, the attack occurs when the fraudulent vehicle directs multiple messages which blocks all potential ways of communication. The outbreak can be accomplished by many attackers simultaneously.

10.2.2 Jamming attack

Jamming attack is one of the unsafe attacks in VANETs security applications and it takes place when one of the suspected vehicle tries to interrupt the streaming communication through various kinds of techniques such as taking in heavy power with equal frequency choice and alert injection.

10.2.3 Platooning attack

It occurs when a large number of unreliable vehicles are located in the same zone or they try to move forward together with the purpose of causing some kind of trouble and removing reliable nodes from the network operation that are restricted for using similar kind of bandwidth.

10.2.4 Betrayal attack

This kind of attack takes place when a reliable vehicle enters into a malicious node and starts in sending fake messages by the node.

10.3 Attack on infotainment applications

The attacks on infotainment applications tend to talk about the issues that are related to the comfort level and safety measures of the passengers.

10.3.1 Illusion attack

Data is received from the antenna and some of the information is collected from the sensor and passed onto the hardware components.it helps in creation of warning messages of the road conditions which help in creation of an illusion of the vehicles that are nearby.

10.3.2 Inject message attack

This type of attack takes place when an unreliable vehicles tries to create a fake message or duplicate the same message or try to create a new type of message by passing in some malicious information and modifying the original message in the network and acts as master node in the inter vehicle communication network.

11 Security and Privacy Related Issues in VANET

Various security schemes have been used to safeguard privacy based on the security mechanisms they use, these schemes can be classified as:

- Pseudonyms coupled with public key infrastructure (PKI)
- Trust-based schemes
- Group signatures

11.1 Pseudonyms coupled with PKI-based schemes

Pseudonyms preserve and protect the privacy of the users. It hides the original identity of the user and avoids any kind of link ability of the identity with a pseudonym. However pseudonyms can reveal the true identity in case the user commits any type of illegal activity hence providing traceability in case of any wrong actions.

The disadvantage of the pseudonym scheme is that the On Board unit has thousands of pseudonyms stored which need to be refreshed on a timely basis. The pseudonyms are continuously changed in order to maintain the privacy of the user.

The pseudonyms need to maintain CRL. CRL stands for Certificate Revocation List. This list keeps information of all the vehicles that are unreliable and untrustworthy. This list needs to be checked continuously which can be both time consuming as well as resource consuming. The certificate authority termed CA links the pseudonyms to the vehicles and hence it must be kept secure in order to maintain the privacy of the users.

11.2 Trust based schemes

Trust-based schemes have been proposed for MANETs. The same has been applied to VANETs as well. In VANETs it includes a large number of nodes and as the vehicles move very quickly the topology keeps on changing quickly. So it becomes difficult to maintain the trustworthiness of the vehicles.

In VANETs the purpose is to increase road safety and hence the decision-making process needs to be very fast due to the high speeds and limited amount of time involved. Trust establishment is done through central authority or by means of security infrastructure. Security infrastructure requires development of a trust score dynamically. The trust score needs to be maintained and checked.

Protection against inside attackers gets difficult in trust based schemes when a group of vehicles combine together to form a network. In order to solve this issue data centric trust schemes have been proposed. In this a false node can be determined easily based upon the information exchange of whether they are forwarding the wrong kind of data. This kind of false node can be reported and ignored.

11.3 Group signatures

For a group of vehicles travelling together at the same speed and direction the Group signatures for the VANETs have been proposed .This proposed model helps in issuing messages and sign the messages with the group signatures in behalf of the entire group. By forming groups privacy can be achieved. The vehicle to vehicle transmission is reduced by means of periodic broadcasts by a single member of the group.

12 Security and Privacy in VCC

The vehicular internet will motivate the longer term of vehicular technology and intelligent transportation systems (ITS). Whether its road safety, infotainment, broadcasting device or self-driving cars, the vehicular internet will lay the motivation for the longer term of road travel. Governments, organisation bodies and corporations are pursuing driver-less or self-driving cars as they're considered to be more trustworthy than humans and, therefore, harmless and safer. The vehicles today aren't just a way of transportation but also are well-appointed with a decent range of sensors that provide valuable data for decision making. If vehicles are allowed to share data that they collect with other vehicles or facilitate for decision-making and harmless driving, and by this means form a vehicular network. However, there are tons at stake in vehicular networks if they're negotiated and compromised. With the risks so high, it's vital that the vehicular networks are protected and made strong to any attack or attempt which will have severe result. The vehicular internet also can be the target of a cyber-attack, which may be overwhelming.

The security and privacy are one among the main characteristics of the vehicular network, which inaugurates, preserves, and enhances the user's expectation within the VC. In particular, the privacy is employed to make sure the communication and knowledge interchange within the VC which is in reliable environment, while the safety is active to guard the vehicular network from warning and attacks, and also from malicious nodes within the network. Olariu et al. considered VCC as a group of vehicles, during which a group of vehicles in VCC could share the vehicle resources like computer resources, the web, computing, and communication to form a predictable cloud computing. Therefore, it leads to cause the same security issues as CC 7almost the VCC and VANETs are partaking the same security issues.

The core security challenges of VCC includes the following:

- Make sure the secure location because the maximum of the applications depend upon location information
- Node's verification and message probity
- Preserve data on cloud from spiteful users
- Privacy of message with cryptography practice.

The security and privacy concerns within the VCC need care from the researchers to develop a strong algorithm which might be ready to stop VCC from different sorts of security threats.

12.1 Security services of vehicular cloud computing

There are mainly five main security requirements. They are:

12.1.1 Confidentiality

It certifies that the main data should not be reveal to the outside nodes.

12.1.2 Integrity

It certifies that message should be valid and the contents of the message are not adjusted during communication process.

12.1.3 Availability

Whenever the vehicle requires some data resources they must be available.

12.1.4 Authentication

In this the VC will be protected by authentication from suspected nodes by checking the user identity and sender address.

12.1.5 Privacy

The vehicles or passengers will be protected from the attackers by the sensitive and confidential information.

12.2 Threats of vehicular cloud computing

The demand of using VCC is increasing very year by the challenges faced by it. Here are some of the threats of Vehicular Cloud Computing.

12.2.1 Denial of service (DOS)

It is a usual attack on vehicular cloud, these attacks happens to make the services unavailable to other cloud users.

12.2.2 Identity spoofing

In this attack the registered user identity and security credentials will be misused by evil user.

12.2.3 Message interferes

This attack happens when the attacker alters the previous messages data to be transmitted. For instance, if the route is crowded, the attacker modifies the data to empty the road which can affect the users to change their driving paths.

12.2.4 Information disclosure

In the absence of data privacy this attack takes place by acquiring the useful data of the system.

12.2.5 Sybil attack

The other vehicular behaviour will get manipulated by these attackers and the vehicle thinks that the information is transmitting from other vehicles. Thus they feel that there is a crowding on the road, so they impose vehicles to change their way and leave the road clear.

Vehicular cloud computing security and privacy related concepts are represented in fig. 4.

12.3 Privacy challenges of vehicular cloud computing

The statistics that's collected from the vehicle's sensors has got to be protected and will only be used after anonymizing it. The worry is that your vehicle should advise you if you're over the directive but shouldn't turn against you, i.e., reporting to the establishments and authorities that you basically went over the speed limit. However, there are many examples when sharing location information with some cloud service providers

might essentially be beneficial for the user, e.g., insurance enterprises might offer to measure back the insurance premiums if such details are shared. There are often similar reasons from other service providers to use vehicle sensor data communally for a few rewards which will actually encourage contribution from the consumers.

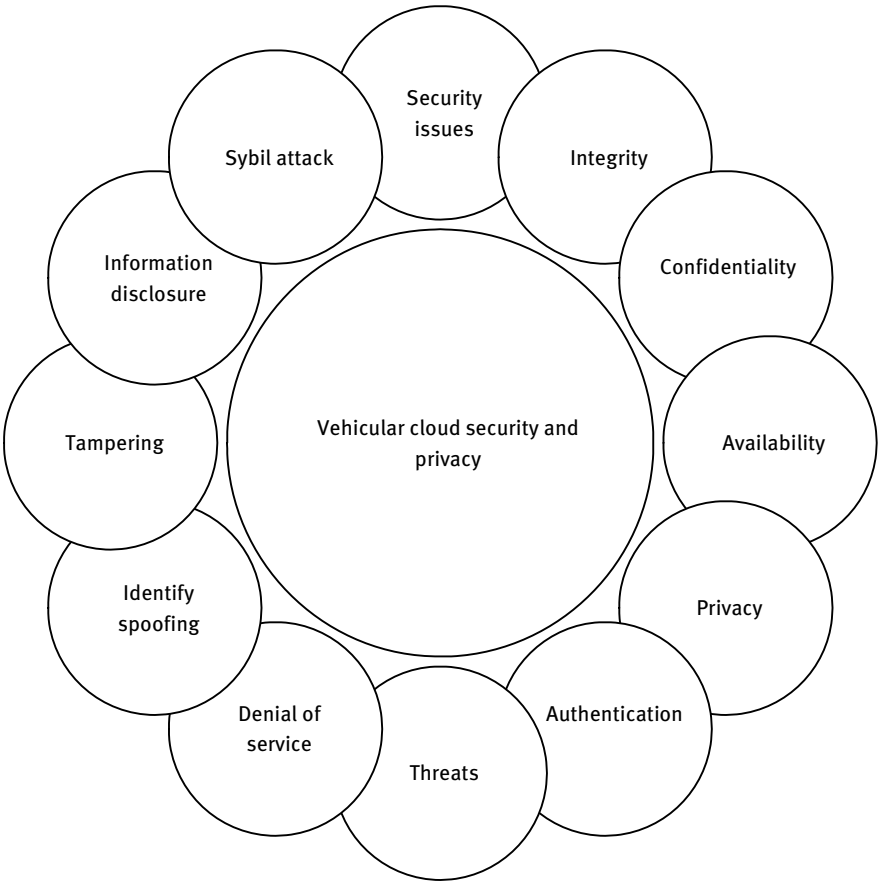

Fig. 4: Security and privacy requirements of vehicular cloud computing

13 Solutions to Security Issues

We recommend a digital identity structure for VANETs by seeing that it's the driving force who is to be held accountable for the vehicle and not the other way around. Therefore, we use the ID of the vehicle and therefore the driver to make a standby digital identity. The two identities are merged into one after verification from two

authorities, i.e., the vehicle registration authority and therefore the driver license authority. Each of the two authorities concerns the user token and secret keys which are then working by the user to get their pseudonym. Therefore, even though the passkey is compromised, the tokens can only be traced by the two authorities and no individual authority can disclose truth uniqueness of the user. The performance of the scheme is enhanced through conditional privacy preservation (ECPP) and pseudonymous authentication-based conditional privacy (PACP).

Python code for anomaly detection- road condition is given in the following code listing.

Listing 1: Python code for anomaly detection- road condition to avoid accidents

```
# Initialize the following variables
P_T_C -->PATH_TO_CKPT,
P_T_L -->PATH_TO_LABEL
N_C -->NUM_CLASSES
#Load the Tensor flow model code into memory
d_graph = tf.Graph()
with d_graph.as_default():
#code to load the model
#Loading label map
l_map = label_map_util.load_labelmap (P_T_L)
catg=l_map_util.convert_label_map_to_categories (l_map, max_num_clas
ses=N_C, use_display_name=True)
c_i = label_map_util.create_category_index (catg)
def load_image_into_numpy_array (image):
#define image and loading details
#To detect images
P_T_T_I_D = '/user/ubuntu/data_set/road_dataset-TF/road_dataset/'
D_T = # set with different road type values
R_L = # set with location values
v_l = []
for loc in R_L:
    img_f = open (# open images in read mode)
    for entry in img_f:
        entry= entry.rstrip ('\n').split ('/')[-1]
        v_l.append (entry)
    img_f.close()
print(str(len (v_l))
with detection_graph.as_default():
  with tf.Session (graph=detection_graph) as sess:
   i_t = detection_graph.get_tensor_by_name ('image_tensor:0')
```

```
   d_b = detection_graph.get_tensor_by_name ('detection_boxes:0')
   d_s = detection_graph.get_tensor_by_name ('detection_scores:0')
   d_c = detection_graph.get_tensor_by_name ('detection_classes:0')
   n_d = detection_graph.get_tensor_by_name ('num_detections:0')
   for img_p in T_I_P:
      img = Image.open (img_path)
      imgs to have shape: [1, None, None, 4]
      img_np_expanded = np.expand_dims (img_np, axis=0)
      (boxes, scores, classes, num) = sess.run (#detection of boxes,
       scores and classes of the images)
      vis_util.visualize_boxes_and_labels_on_image_array (
          #set the image characteristics)
#Plot the figure using figure and imshow
```

14 Conclusion

According to our report We conclude that the VANETs becomes very fashionable within the traffic management system, which aims to make sure the security of human lives on the road and supply comfort to travellers by broadcasting safety messages among vehicles. As these safety messages are transmit in an open-approach environment that creates VANETs more permitting to the attacks, a strong security algorithm must be designed for set about security threats and attacks which could make sure the secure transmission within the VANETs and VCC.

In this report, we first present the introduction of the VANETs and its applications. Then, about the VANET and clouds in that we described briefly about VANET within cloud, vehicular cloud, Private cloud and autonomous vehicle. Second, we've discussed about the vehicle platoon/swarm and then the applications of vehicular cloud computing. Third, we've discussed the VANET characteristics explained followed by the safety and privacy problems with the VCC intimately. Finally, we've presented some issues associated with VANETs and VCC that are considered as open research challenges during a vehicular network.

The research management for VANETs basis on the safety and privacy issues like trust model and cryptography-based technique to validate safety messages. Based on these techniques, researchers could design a strong security system, which may be ready to prevent VANETs from different sorts of security threats and attacks. In addition to VANETs, the VCC residue within the starting stage and expected to supply an ideal solution to guard the network from different type of threats and improve the organization of the traffic management system. In our opinion, supported the prevailing VCC procedures, architectures, and practices, an improved algorithm might be designed to scale back the trust and privacy issues in VCC.

15 References

[1] Coady Y, Hohlfeld O, Kempf J, McGeer R, Schmid S, Distributed cloud computing: applications, Status Quo, and Challenges, SIGCOMM Comput. Commun. Rev, 2015, 45, 2, 38–43, DOI:https://doi.org/10.1145/2766330.2766337

[2] Kliazovich D, Arzo S, Granelli F, Bouvry P, Samee U, e-STAB: Energy-efficient scheduling for cloud computing applications with traffic load balancing, 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, Beijing, China, 2013, pp. 7-13, doi: 10.1109/GreenCom-iThings-CPSCom.2013.28.

[3] Nayak J, Naik B, Jena A, Barik R, Das H, Nature inspired optimizations in cloud computing: applications and challenges, Mishra B, Das H, Dehuri S, Jagadev A, Cloud Computing for Optimization: Foundations, Applications, and Challenges, Studies in Big Data, 2018, vol 39, Springer, Cham, https://doi.org/10.1007/978-3-319-73676-1_1

[4] Bahga A, Madisetti V, Synthetic workload generation for cloud computing applications, Journal of Software Engineering and Applications, 2011, Vol. 4 No. 7, pp. 396-410, doi: 10.4236/jsea.2011.47046

[5] Heap-Yih C, John W, Xiangyu W, An explanatory case study on cloud computing applications in the built environment, Automation in Construction, 204, Volume 44, Pages 152-162, ISSN 0926- 805, https://doi.org/10.1016/j.autcon.2014.04.010

[6] Potluri S, Subbarao K, Quality of Service based task scheduling algorithms in cloud computing, International Journal of Electrical and Computer Engineering, 2017, Vol. 7, No. 2, PP: 1088-1095

[7] Potluri S, Subbarao K, Improved quality of service-based cloud service ranking and recommendation model, TELKOMNIKA Telecommunication, Computing, Electronics and Control, 2020, Vol. 18, No. 3, pp. 1252~1258 ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018 DOI: 10.12928/TELKOMNIKA.v18i3.11915

[8] Potluri S, Subbarao K, A hybrid PSO based task selection and recommended system for cloud data, test engineering and management, 2020, Vol-83, ISSN: 0193-4120 PP: 10210 – 10217

[9] Potluri S, Subbarao K, hybrid self-adaptive PSO and QoS based machine learning model for cloud service data, International Journal of Control and Automation, 2020, Vol. 13, No. 2s, pp. 36 - 50, ISSN: 2005- 4297

[10] Potluri S, Subbarao K, Optimization model for QoS based Task scheduling in cloud computing environment, International Journal of Electrical, Electronics and Computer Systems, 2020, Vol. 18 , No 2, pp. 1081-1088, ISSN: 2502-4752, DOI: 10.11591/ijeecs.v18.i2.pp1081-1088

[11] Whaiduzzaman M, Sookhak M, Abdullah G, Buyya R, A survey on vehicular cloud computing, Journal of Network and Computer Applications, 2014, Volume 40, Pages 325-344, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2013.08.004

[12] Qin Y, Huang D, Zhang X, VehiCloud: Cloud computing facilitating routing in vehicular networks, 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, UK, 2012, pp. 1438-1445, doi: 10.1109/TrustCom.2012.16

[13] Jiau M, Huang S, Hwang J, Vasilakos A, Multimedia services in cloud-based vehicular networks, IEEE Intelligent Transportation Systems Magazine, 2015, vol. 7, no. 3, pp. 62-79, doi: 10.1109/MITS.2015.2417974

[14] Bitam S, Mellouk A, Zeadally S, VANET-cloud: a generic cloud computing model for vehicular Ad Hoc networks, IEEE Wireless Communications, 2015, vol. 22, no. 1, pp. 96-102, doi: 10.1109/MWC.2015.7054724

[15] Zhao J, Li Q, Gong Y, Zhang K, Computation offloading and resource allocation for cloud assisted mobile edge computing in vehicular networks, IEEE Transactions on Vehicular Technology, 2019, vol. 68, no. 8, pp. 7944-7956, Aug. 2019, doi: 10.1109/TVT.2019.2917890

[16] Euisin L, Eun-Kyu L, Mario G, Soon Y, Vehicular cloud networking: architecture and design principles, IEEE Communications Magazine, 2014, vol. 52, no. 2, pp. 148-155, doi: 10.1109/MCOM.2014.6736756

[17] Alazawi Z, Altowaijri S, Mehmood R, Abdljabar M, Intelligent disaster management system based on cloud-enabled vehicular networks, 2011 11th International Conference on ITS Telecommunications, St. Petersburg, Russia, 2011, pp. 361-368, doi: 10.1109/ITST.2011.6060083

[18] Yu R, Zhang Y, Gjessing S, Xia W, Yang K, Toward cloud-based vehicular networks with efficient resource management, IEEE Network, 2013, vol. 27, no. 5, pp. 48-55, doi: 10.1109/MNET.2013.6616115

[19] Hassan A, Luong T, Jin W, Sungyoung L, Saad Q, V-Cloud: vehicular cyber-physical systems and cloud computing, In Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies, Association for Computing Machinery, New York, NY, USA,2011, Article 165, 1–5, DOI:https://doi.org/10.1145/2093698.2093863

Sirisha Potluri, Sachi Nandan Mohanty, A. D. Sriram Kumar, D. Maheswari, B. Rahini

Cloud Manufacturing Service: A Secure and Protected Communication System

Abstract: Cloud computing is the one of the most important technology in the current world and it has the high ability to reduce the cost. Cloud computing allows cloud users to put their information, data and requests on the cloud service provides like Azure, Amazon AWS and Google suit. Cloud provides computing software like a development platform where you can create or develop your own applications. The cloud consumers can use all these resources provided by cloud service provider from anywhere in the world through the internet facility. Using the cloud there are many advantages, and also many security challenges for the organizations regarding cloud based data storage solutions. Cloud manufacturing is a novel manufacturing architype developed from prevailing innovative manufacturing prototypes and enterprise level information expertise under the provision of cloud computing, IoT, virtualization technology and service oriented computing, and cutting-edge computing technologies and expertise. Manufacturing as a service is an advanced manufacturing architype developed from the existing cutting-edge manufacturing models such as ASP, AM, NM and MGrid. This work is to study and discuss about security and privacy issues and solutions in cloud based manufacturing.

Keywords: Cloud Computing, Cloud Security, Cloud Manufacturing, Cloud Privacy, Internet of Things, Manufacturing as a Service, Encryption, Decryption

Sirisha Potluri, Department of CSE, IcfaiTech (Faculty of Science and Technology), ICFAI Foundation for Higher Education, Donthanapally, Shankarpalli Road, Hyderabad, Telangana 501203, India, sirisha.vegunta@gmail.com
Sachi Nandan Mohanty, Department of Computer Engineering, College of Engineering Pune, Wellesley Rd, Shivajinagar, Pune, Maharashtra 411005, India, sachinandan09@gmail.com
A. D. Sriram Kumar, Department of CSE, IcfaiTech (Faculty of Science and Technology), ICFAI Foundation for Higher Education, Donthanapally, Shankarpalli Road, Hyderabad, Telangana 501203, India, annasriram914@gmail.com
D. Maheswari, Department of CSE, IcfaiTech (Faculty of Science and Technology), ICFAI Foundation for Higher Education, Donthanapally, Shankarpalli Road, Hyderabad, Telangana 501203, India, maheshwari.dantuluri17@ifheindia.org
B. Rahini, Department of CSE, IcfaiTech (Faculty of Science and Technology), ICFAI Foundation for Higher Education, Donthanapally, Shankarpalli Road, Hyderabad, Telangana 501203, India, rahini890@gmail.com

https://doi.org/10.1515/9783110732573-009

1 Introduction

Cloud computing is a great blessing for the very fast grow in the world of information technology. Cloud computing is delivering the required and on demand resources for their customers through the internet such as data storage, servers, data bases, networking and software. It is a sophisticated architecture which stores the data on remote servers and it can be accessed through the internet. Cloud based storage allows us to store all the data in a safe and secure way and we can access it whenever we required from anywhere just through the internet. Cloud computing uses the payment option namely pay as you go basis means pay for what you use. Many cloud providers in the marketplace namely Amazon web services, Google cloud platform and Azure are effectively providing on demand resources to the cloud consumers.

The computing resources are pooled together by the cloud service provider over the infrastructure and the same can be provisioned to the users when they need them. The cloud users or consumers will be charged and billed only for what they have used or consumed from the cloud. Significant advantages of the cloud computing includes enhanced privacy, improved security, reduced costs, agility based development, location transparency, extremely scalable, easy maintenance, device independence, high performance, flexible and increase in productivity. To safeguard the data and information which is stored by the cloud service providers integrity, availability and confidentiality is maintained by them.

Cloud manufacturing is also known as a novel manufacturing architype that is developed from an existing and cutting-edge manufacturing models. The idea of cloud manufacturing was originally recommended by a research group that was headed by Prof. Bo Hu Li and Prof. Lin Zhang from China in the year 2009. After that good amount of related research and discussions are being conducted and some similar definitions to cloud manufacturing were introduced [1-5].

2 Manufacturing Cloud Provision Models

In the current market there are three types of services which are offered by the cloud computing namely infrastructure as a service, software as a service and platform as a service.

IaaS- Infrastructure as a service means that it provides business offers and services based on pay as you go model. This can avoid investing in expensive storages, servers, maintenance and gives users cloud based instead, so it delivers all those services on the internet. The main advantage of the IaaS is that it provides highly scalable services to the cloud users based on their demand. It ensures stability, reliability and supportability, better security, quick response and rapid innovation.

SaaS- Software as a service makes use of all the software services through the internet, they are like paid and use purpose. By using this SaaS, we do not need to install any other kind of software applications on your computer. All these software applications are available on the cloud and we can access them through the internet when you require them.

PaaS- Platform as a service is one of the cloud computing service which uses virtualization technology for the development platform for the cloud users and the organizations. This platform is also include the memory, databases, computing, storage, and also some other application development services. PaaS is mostly useful for the environment for developing and the testing the applications. The main advantages of this platform as a service is that it has no need to purchase hardware, no need to spend more time, it will be speed up your applications, any person can just login and use the applications from anywhere, and has high security for the data being stored in it and no need to worry for the data loss [6-9].

3 Manufacturing Cloud Organization Models

Depending upon the deployment, cloud is divided into four models namely public cloud, private cloud, hybrid cloud and community cloud.

Public Cloud- Public cloud provides all the resources to the cloud users and the resources can be accessed by everyone through the internet. Examples for the public cloud is Microsoft Azure, in public cloud you can share same storage and hardware with other organisations. The key benefits of the public cloud are security, flexibility, controllability and cost effectiveness.

Private Cloud- Private cloud allows the resources only with the specific or selected users instead of using them by all public users. It solves the security issues of public cloud with the help of dedicated resource usage. The main advantages of this private cloud are increase in security, efficient performance and competent capability.

Hybrid Cloud- Hybrid cloud is a combination of both public cloud and the private cloud. This type of cloud suits when an organisation uses the public cloud and private for various requirements and demands. The advantages of the hybrid cloud are flexibility, backup clouds, cost saving, security for the sensitive data.

Community Cloud- Community cloud shares the computing services to the mainly targeted or some organisations. This type of cloud computing is also used for the business organisations, research organisations and tenders and also heads of trading firms. The main advantage of this community cloud are availability, reliability, security and improved service provisioning [10-13].

Manufacturing cloud provision and organization models are represented in the following fig. 1.

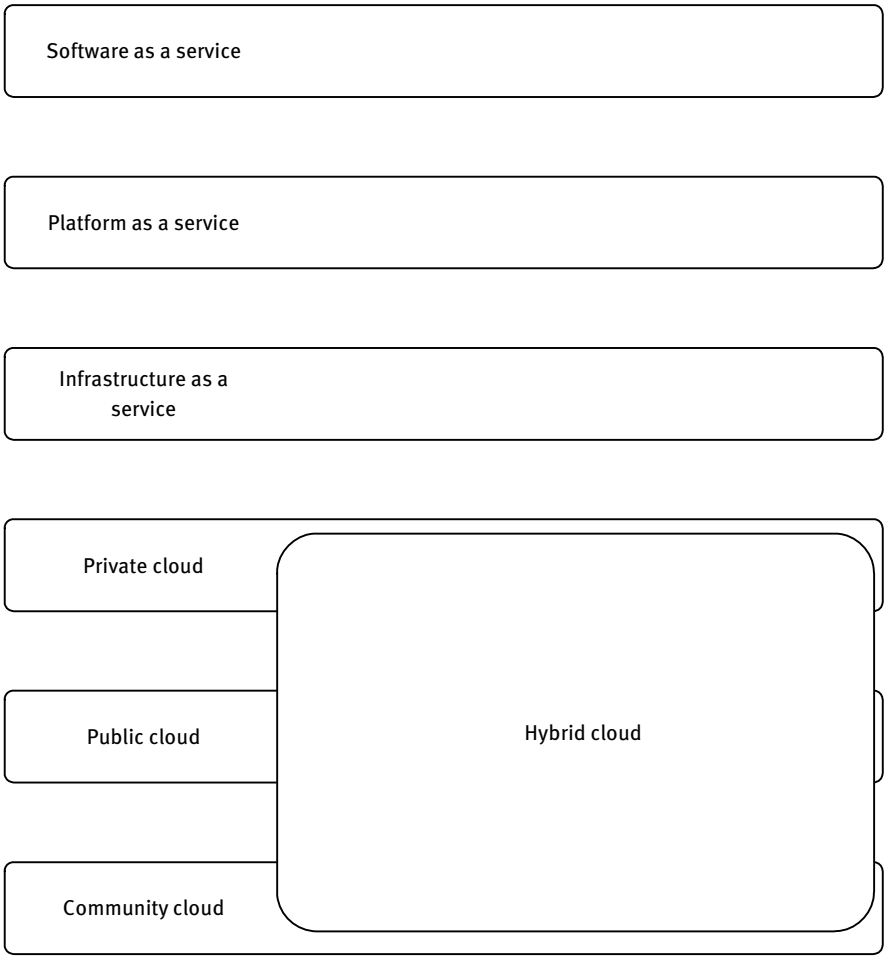

Fig. 1: Manufacturing cloud provision and organization models

4 Cloud Manufacturing Paradigms

Cloud manufacturing is a parallel, thin, networked, interacted and distributed system that includes an interlinked and integrated virtualized service pool of manufacturing resources. This paradigm has the ability of intelligent management and controlling of on demand use of services by providing solutions for all kinds of users that are included in entire lifecycle of manufacturing [14-16]. The idea of cloud manufacturing implies to a paradigm which includes the entire lifecycle of a product like production, simulation, designing, test and maintenance. Applications of cloud based manufacturing are fabricated metal products, automobile manufacturing, housing, building

and furniture manufacturing, textiles, semiconductors and computers manufacturing, transportation system manufacturing, distribution and warehousing, plastic and rubber products, heavy manufacturing and electronics manufacturing are shown in fig. 2.

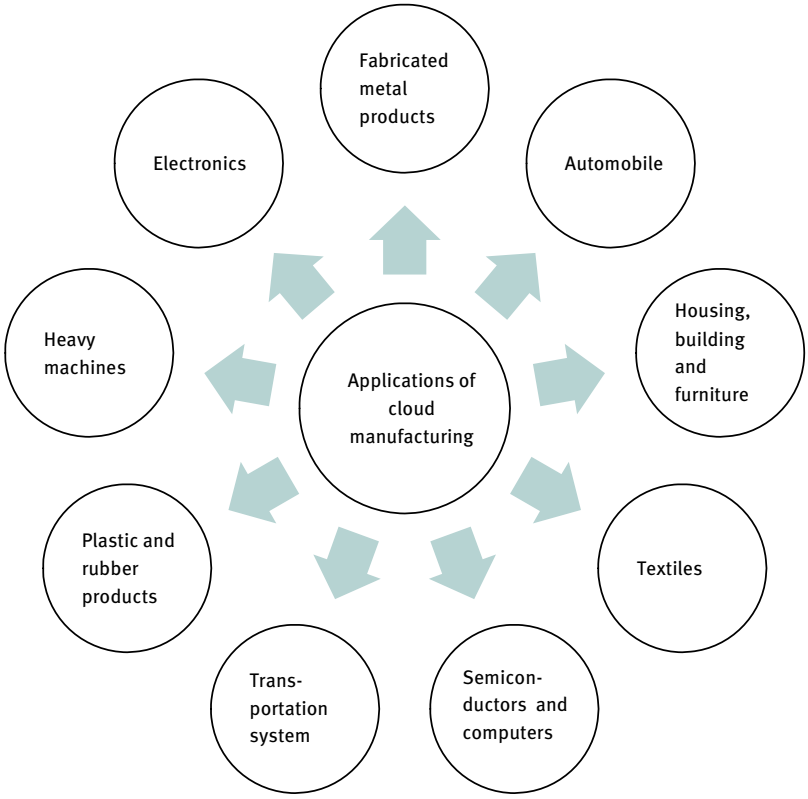

Fig. 2: Applications of cloud based manufacturing

5 Benefits of Cloud Manufacturing

Benefits of cloud manufacturing are:

5.1 Scalability

Cloud centred software is a pay-as-you-go system, it means that during the demanding times of the day/month/year the number of subscriptions that are used can be increased. This helps to optimize the expenditures and keeps the spending predictable.

5.2 Increased uptime

Cloud enables its users to continuously have the latest and state of the art version of the software for its users. So, at whatever time the software is improved or updated for better quality, everyone is benefitted by getting the updates immediately and right away.

5.3 Standardization

Standardization improves the consistency of the resource utilization and usage by streamlining the business practices and creation of standardization across the entire operation.

5.4 Faster implementation

Due to faster implementation of cloud customer requirements, time and money are saved.

5.5 Agility

Due to agility entire manufacturing process involves less operational cost by using cloud manufacturing model.

Cloud computing system can be divided into three categories according to manufacturing resources are follows:

- Service oriented and adapted input
- Operating and working platform of the manufacturing resource
- Service oriented and adapted output

There are three categories of key stake holders in cloud manufacturing system. They are:

- Providers
- Operators
- Consumers

Providers will publish their resources to cloud manufacturing platform, the operators manage all aspects of platform that are relevant to the platform running and operation, and the consumers requests the services from cloud platform.

A cloud based manufacturing platform consists of five layers as shown in fig. 3. They are:

- Business planning

- Manufacturing operations management
- Automation and control
- Sensors and actuators
- Production process

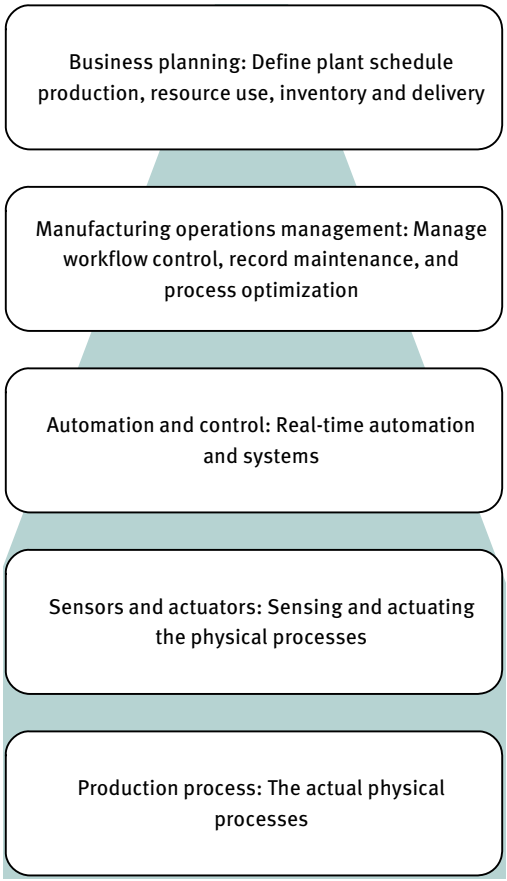

Fig. 3: Layer wise architecture of cloud based manufacturing platform

Cloud manufacturing is facing many challenges due to its integration with many technologies. Cloud computing ensures high performance using semantic web, internet of things and embedded systems. Several technical issues must be solved such as cloud management engines, collaboration between cloud manufacturing applications, knowledge base resource clouding and visualization and user interface in cloud computing environments [17-18].

6 Security and Privacy Aspects of Cloud Manufacturing

Security in cloud computing is a set of control based integrated technologies & policies aimed to stick with the regular organizations, rules and protect/guard data application and cloud technology infrastructure. Due to efficient resource sharing, cloud security gives main problem to identity management, access control and privacy. The data in the cloud should be stored in an encrypted form. It processes the security control in cloud and provides customer data security, compliance, and privacy with necessary regulations.

6.1 Security challenges in cloud manufacturing

Cloud provides all its resources to many organisations in the subscription manner. Though it has many advantages cloud needs to address many challenges as given below.

6.1.1 Reliability

The consumers' data are stored in third party's server. They do not know where or which location their data are being stored. They are not aware of what security mechanisms provided to safeguard their data.

6.1.2 Privacy

All the cloud users store their data in the cloud and that is stored in some of the physical machines in various places around the world. All the data is being transferred through the internet.

6.1.3 Data loss

Data loss is the one of the most security challenge in the cloud computing. If any cloud user stores the important data in the cloud, we need to concern about the security issues. If the data is lost through natural disasters or accidents or through the DDoS it leads to disastrous to the organisation.

6.1.4 Bandwidth

When there is high demand of the resources or high volume of data is to be stored, then high bandwidth is required.

6.1.5 Availability

At sometimes, when the huge amounts of resources are to be served at a time, then the cloud becomes unable to give all the consumers' demands.

6.1.6 Integrity

Cloud need to ensure the correctness and trustworthy of the consumers data. The data should not be modified, maliciously fabricated, deliberately deleted or tampered.

6.1.7 DoS

Denial of Service attack thrown by malicious users by selecting/choosing a victim machine and by sending the bulk requests to the virtual machines at the same time, then the services will not be made available to the reliable and true users.

6.1.8 Authentication

Every cloud user should be checked and authenticated before accessing the cloud resources.

6.1.9 Access control

The cloud users or consumers need to be categorized and given permissions according to the type of the cloud users.

Cloud service providers like Google cloud platform, Microsoft Azure, Amazon web services are providing the best sources to the users to shift to the cloud computing. And users need not worry about their data security, because it's being maintained by set of policies and protocols, virtual machines and data security as per the rules and regulations.

6.2 Significant factors effecting security in cloud system

Significant factors effecting security in cloud system are confidentiality, integrity, and availability.

6.2.1 Confidentiality

Confidentiality is very important using which our data is not accessible to unauthorized parties. It means that the sensitive data is accessible to only the authorized persons. A failure in maintaining confidentiality means that unauthorized person has the access to all the required sources provided by the provider which will be caused due to intentional behaviour or by accident. This failure is known as confidentiality failure or breach. Once the confidential data is leaked like bank details it leads to high risks.

Requirements of confidentiality are divided into two categories namely data confidentiality and virtualization confidentiality.

6.2.1.1 Data confidentiality

Cloud providers provide many online services to store the cloud user data. This may sometimes result in potential loss of data security and confidentiality. When the data is shared in a group using a distributed cloud storage service, the client should get periodic update regarding the data changes by any user in the group. They are many more interesting things by knowing the contents of the cloud user as well as the cloud user's access account and privilege information.

6.2.1.2 Virtualization confidentiality

In infrastructure as a service, cloud service provider hosts virtual machines when there is a requirement from cloud users or customers. In cloud system, anyone with the privileged access can read or change the deployed service. This means that the total virtualization layer induces some security issues by considering all cloud security related issues. Virtual machines allows elastic scaling, fault tolerance, hardware pooling, easy maintenance, load balancing, and resource maintenance.

6.2.2 Integrity

Integrity is asset that promises the data or information is not been modified by any third-party personnel who is not an authorized individual for such activity. Thus the correctness and accuracy of an asset is with respect to its owner to ensure integrity. Usually delete, edit, and append operations are believed by the change in integrity.

Consequently all the web related attacks are highly prevailing in cloud environment that can alter or change the contents of the virtual machine metadata, databases, user files/log files, and WSDL files.

Integrity requirements are divided into two categories namely data integrity and virtualization integrity.

6.2.2.1 Data integrity

Cloud scheme allows decent number of data centric operations and tasks with very huge data requirements where huge refers to terabytes and petabytes. Thus data reliability challenges related with the PaaS (platform as a service), DaaS (data as a service) etc. needs to be handled very carefully. Some of the cloud specific data integrity issues are as follows:

- Data transfer/outsourcing
- SQL injection
- Cross scripting
- Metadata Spoofing attack
- Wrapping attack

6.2.2.2 Virtualization Integrity

As we have discussed in the earlier section, the virtualization layer it has of its own security related challenges and issues which are not limited with privacy and security but also integrity of the virtual machines. Some of the cloud specific virtualization integrity issues are as follows:

- Cloud Service Provider administrators
- Virtual Machine replication
- Virtual Machine rollback
- Virtual Machine escape
- VM hopping

6.2.3 Availability

Availability is one of the significant aspects of security that has to be maintained and preserved by the cloud service provider. Diverse business enterprises and initiatives who use the cloud based services to serve and work for their customers must guarantee the highest availability of these services. Even a smallest amount of downtime or stoppage of the service can result into a large financial loss which is irredeemable.

This availability requirements are divided into two categories namely data availability and virtualization availability

6.2.3.1 Data availability

One of the significant issues affecting the cloud data availability is DDoS attack. Different types of DDoS are recognised in the cloud environment are as follows.

- Denial of Service
- Indirect Denial of Service
- Natural disasters

6.2.3.2 Virtualization availability

Virtualization technology allows highest availability of resources and detects DDoS attacks trough intrusion detection sensors. IBM smart cloud enterprise brought the concept of virtual IP addresses for ensuring high availability of the cloud service when there is an IP failover.

7 Comparison of Traditional/Conventional Manufacturing and Cloud Manufacturing

Comparison of traditional/conventional manufacturing and cloud manufacturing are given fig. 4 and fig. 5.

Traditional manufacturing suffers with the following limitations and are addressed by cloud manufacturing.

- Restricted and dedicated resources
- Static routing
- No interconnection and integration
- Independent control
- Isolated information
- Independent module setup
- Discrete work groups
- Lack of automation
- More manual work

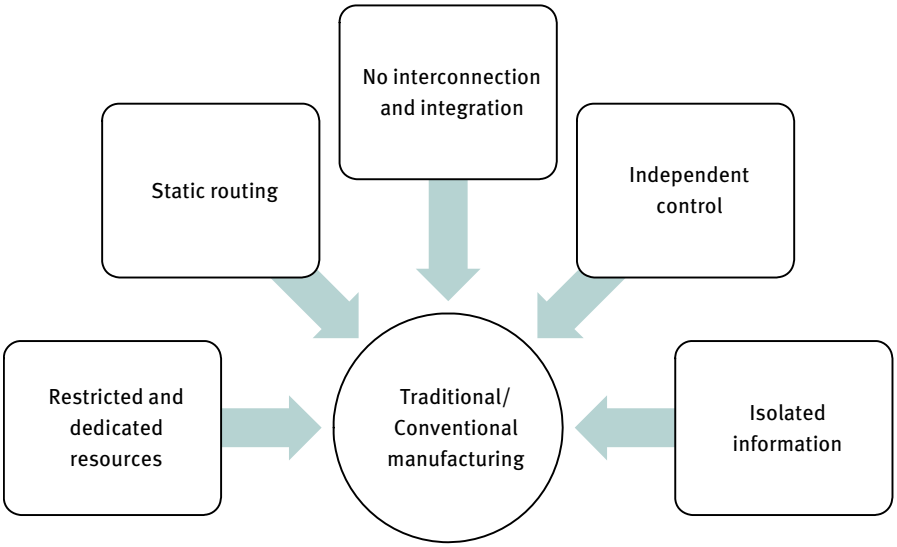

Fig. 4: Limitations of traditional/conventional manufacturing

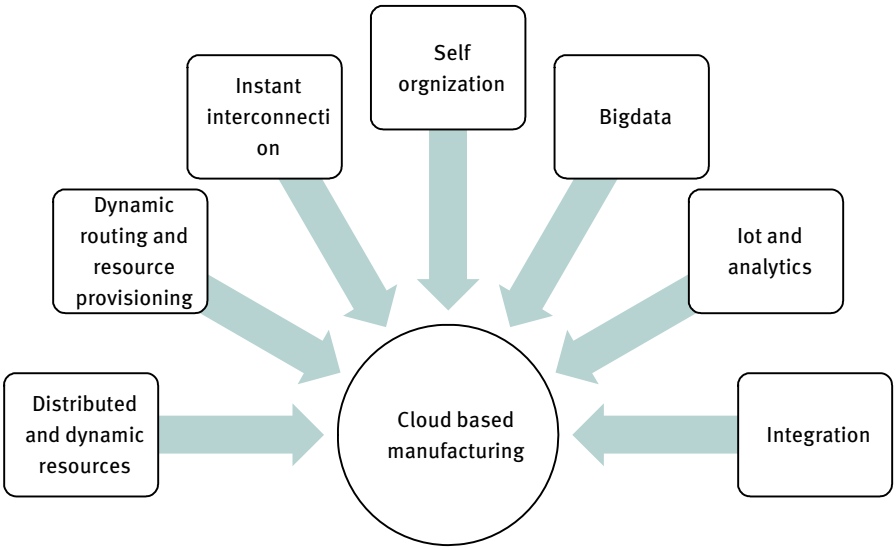

Fig. 5: Advantages of cloud manufacturing

8 Secure Cloud Manufacturing Models

Table 1 is showing the analysis of secure cloud manufacturing models.

Tab. 1: Secure cloud manufacturing models

S.No	Authors	Secure cloud manufacturing model and its key practices
1	Carsten Ellwein, Oliver Riedel, Olga Meyer, Daniel Schel [19]	The manufacturing process observe frequent changes due latest current trends and technologies of digitalization such as IoT, cloud computing and data analytics. Cloud manufacturing model does influence product production and manufacturing life cycle. Key practices: 1. Digitalization 2. Industrial Internet of Things 3. Cloud manufacturing 4. Secure technology stack 5. Service-oriented architecture for modular computing 6. Secured rent and produce (RnP) as a service 7. Integrated computer aided manufacturing 8. Computerized numerical control
2	Zhi Li, Ali Vatankhah Barenji, George Q. Huang [20]	New evolving manufacturing prototypes such as cloud based manufacturing, IoT facilitated manufacturing and service-oriented architecture, have observed many benefits to the manufacturing industry. Key practices: 1. Distributed network for cloud manufacturing 2. Blackchain technology to ensure security 3. Secure data sharing 4. IoT enabled manufacturing and service-oriented manufacturing 5. Distributed peer to peer network architecture to preserve security and privacy in cloud manufacturing (CMfg) 6. Blockchain based cloud manufacturing (BCmfg) allows secure data sharing 7. Five layer integrated model is proposed to achieve more security and scalability
3	Christian Esposito, Aniello Castiglione, Ben Martini, Kim-Kwang Raymond Choo [21]	Smart manufacturing upturns effectiveness and competence through interconnection and collaboration among organizations or among physical/logical/human resources within a single company. Latest improvements due to industry 4.0 supports collaboration, integration and cooperation among the organization for better

S.No	Authors	Secure cloud manufacturing model and its key practices
		resource sharing and usage Key practices: 1. Collaborative networked manufacturing 2. Layered secure architecture of cloud manufacturing 3. Four phases of key management for secure cloud manufacturing 4. Secure cloud service for defending against data breaches in cloud manufacturing 5. Networked manufacturing model
4	Haibo Yi [22]	Cloud manufacturing has been acknowledged extensive attentions everywhere the world. The expertise of cloud manufacturing integrates services-oriented practices as well as manufacturing practices based on cloud computing. With the assistance of the cloud computing platforms, the manufacturing services are provided efficient secure solutions to make it as a most popular choice. Key practices: 1. Post-quantum asymmetric-key encryption scheme for data security 2. Post-quantum public-key signature generation for authentication security 3. Post-quantum secure communication system for secure and efficient cloud manufacturing 4. Safeguarding cloud manufacturing communication 5. Secure and privacy preserving encryption and decryption system
5	Florin Anton, Theodor Borangiu, Silviu Răileanu, Silvia Anton, Nick Ivănescu, Iulia Iacob [23]	Cloud systems ensuring more production trough industry 4.0 solutions, integrating shop-floor processes and managing higher-level enterprise modules. Key practices: 1. Cloud based manufacturing system integration 2. Remote access and control to manufacturing system 3. VM based custom configured cloud

9 Cloud manufacturing Life Cycle: An Efficient Integrated Approach

IoT, data analytics, big data, self-organization, and efficient resource utilization is achieved through efficient integration of cloud manufacturing as shown in fig. 6.

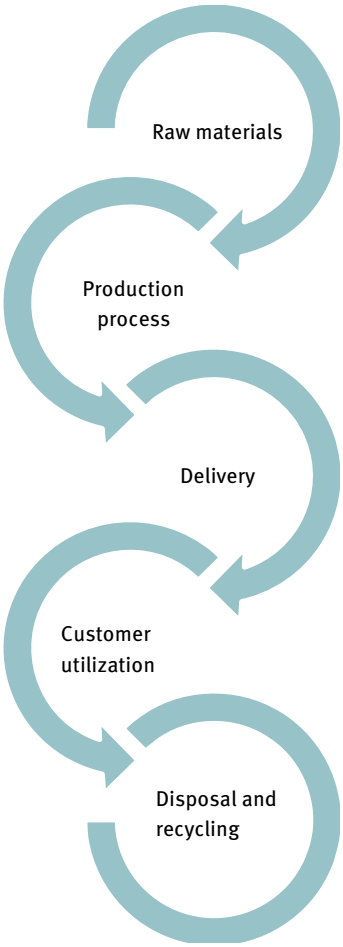

Fig. 6: Cloud manufacturing- Integrated approach

10 Proposed Secured Cloud Manufacturing Model Architecture

The proposed architecture is illustrated in fig. 7. The proposed model has asymmetric-key encryption scheme for data security, public-key signature generation for authentication security and secure communication sys-tem for secure and efficient cloud manufacturing to safeguard cloud manufacturing system communication and data security.

Different keys are used to encrypt and decrypt the data at sender and receiver side. With improved encryption mechanism plain text is converted into cipher text. Using efficient decryption mechanism cipher text is converted in to plain text.

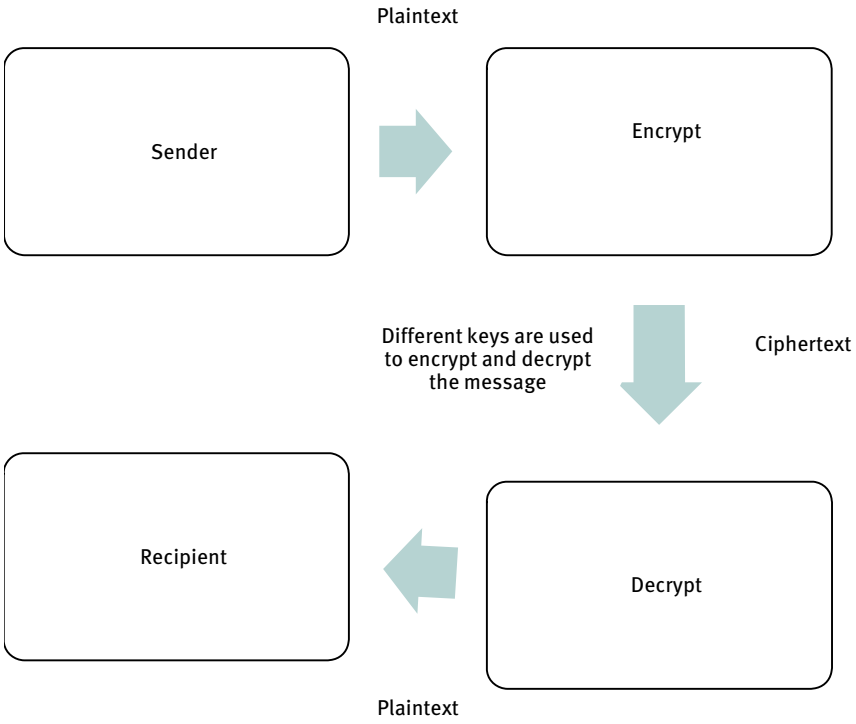

Fig. 7: Architecture of secure cloud manufacturing model

The following code shows secure data encryption using python platform.

Listing 1: Secure data encryption: Python code

```
# Key encapsulation
from pprint import pprint
import oqs
km = oqs.get_enabled_KEM_mechanisms()
pprint(km, compact="True")
kmmech = "DEFAULT"
with oqs.KeyEncapsulation(kmmech) as clnt:
    with oqs.KeyEncapsulation(kmmech) as srv:
        pprint(clnt.details)
        p_k = clnt.generate_keypair()
        c_txt, sh_s_s = srv.encap_secret(public_key)
        sh_s_c = clnt.decap_secret(ciphertext)
        print(sh_s_c)
# Random number generation
import platform, oqs.rand as oqsrand
ornd.randombytes_nist_kat_init_256bit(bytes(entropy_seed))
#Check system settings and switch the algorithm
# Key signature generation
s_sig = oqs.get_enabled_sig_mechanisms()
pprint(s_sig, compact="True")
msg = "This is message from key generation message".encode()
s_a = "DEFAULT"
with oqs.Signature(s_a) as i_sig:
    with oqs.Signature(sigalg) as i_ver:
        pprint(i_sig.details)
        s_p_k = i_sig.generate_keypair()
        sgn = i_sig.sign(msg)
        is_v = i_ver.verify(msg, sgn, s_p_k)
#Post quantum key encryption
pip install pynewhope
from pynewhope import newhope
p_key, message1 = newhope.keygen()
s_key, message2 = newhope.sharedB(message1)
sh_key = newhope.sharedA(messsage2, p_key)
if sh_key == s_key:
    print("Success")
else:
    print("Fail")
```

11 Conclusion

Mobile and instant communication for machines is increasing the importance of the manufacturing industry. Smooth movement of operations, improving production, automation of production life cycle, cloud based security, IoT based services and offerings, service oriented computing paradigms, advanced encryption and decryption mechanisms, faster growth and platform safety are driving cloud manufacturing to a next high. Cloud based manufacturing ensures reduced costs, on demand delivery, efficient data management and efficient management of human resources through competent practices and protocols.

12 References

[1] Tao F, Zhang L, Venkatesh V, Luo Y, Cheng Y, Cloud manufacturing: a computing and service-oriented manufacturing model, Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture, 2011, 225(10), 1969-1976, doi:10.1177/0954405411405575

[2] Li B, Zhang L, Ren L, Chai X, Tao F, Luo Y, Wang Y, Yin C, Huang G, Zhao X, Further discussion on cloud manufacturing, Comput. Integr. Manuf. Syst, 2011, 17(3), pp. 449–457

[3] Ren L, Cui J, Li N, Wu Q, Ma C, Teng D, Zhang L, Cloud-based intelligent user interface for cloud manufacturing: model, technology, and application, ASME, J. Manuf. Sci. Eng, August 2015, 137(4), 040910, https://doi.org/10.1115/1.4030332

[4] Wu D, Thames J, Rosen W, Schaefer D, Towards a cloud-based design and manufacturing paradigm: looking backward, looking forward, Proceedings of the ASME 2012 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference, Volume 2: 32nd Computers and Information in Engineering Conference, Parts A and B, Chicago, Illinois, USA, 2012, pp. 315-328, https://doi.org/10.1115/DETC2012-70780

[5] Wu D, Greer J, Rosen W, Schaefer D, Cloud manufacturing: strategic vision and state-of-the-art, J. Manuf. Syst, 2013, 32(4), pp. 564–579, 10.1016/j.jmsy.2013.04.008

[6] Xu X, From cloud computing to cloud manufacturing, Rob. Comput. Integr. Manuf, 2012, 28(1), pp. 75–86, 10.1016/j.rcim.2011.07.002

[7] Dazhong W, Matthew J, David W, Dirk S, Cloud manufacturing: strategic vision and state-of-the-art, Journal of Manufacturing Systems, 2013, Volume 32, Issue 4, Pages 564-579, ISSN 0278-6125, https://doi.org/10.1016/j.jmsy.2013.04.008

[8] Lin Z, Yongliang L, Fei T, Bo H, Lei R, Xuesong Z, Hua G, Ying C, Anrui H, Yongkui L, Cloud manufacturing: a new manufacturing paradigm, Enterprise Information Systems, 2014, 8:2, 167-187, DOI: 10.1080/17517575.2012.683812

[9] Lei R, Lin Z, Fei T, Chun Z, Xudong C, Xinpei Z, Cloud manufacturing: from concept to practice, Enterprise Information Systems, 2015, 9:2, 186-209, DOI: 10.1080/17517575.2013.839055

[10] Lihui W, Machine availability monitoring and machining process planning towards cloud manufacturing, CIRP Journal of Manufacturing Science and Technology, 2013, Volume 6, Issue 4, Pages 263-273, ISSN 1755-5817, https://doi.org/10.1016/j.cirpj.2013.07.001

[11] Petri H, Duy P, Yuqiuge H, Cloud manufacturing – scheduling as a service for sheet metal manufacturing, Computers & Operations Research, 2019, Volume 110, Pages 208-219, ISSN 0305-0548, https://doi.org/10.1016/j.cor.2018.06.002

[12] Potluri S, Primary methods to address the data security problems in cloud computing, The IUP Journal of Computer Sciences, 2016, Vol. X, Nos. 1 & 2, pp. 18-24, 2016
[13] Avinash M, Potluri S, A study on technologies in cloud-based design and manufacturing, International Journal of Mechanical and Production Engineering Research and Development (IJMPERD), 2018, Volume 8, Issue 6, PP: 187-192, ISSN(P): 2249-6890; ISSN(E): 2249-8001
[14] Potluri S, Subbarao K, Quality of service-based cloud models in manufacturing process automation, Innovations in Computer Science and Engineering. Lecture Notes in Networks and Systems, 2019, vol 32, PP: 231-240, Springer, Singapore. https://doi.org/10.1007/978-981-10-8201-6_26
[15] Zhang Y, Zhang G, Liu Y, et al., Research on services encapsulation and virtualization access model of machine for cloud manufacturing, 2017, J Intell Manuf, 28, 1109–1123, https://doi.org/10.1007/s10845-015-1064-2
[14] Wang X, Mohammad G, Lihui W, Manufacturing System on the Cloud: a case study on cloud-based process planning, Procedia CIRP, 2017, Volume 63, Pages 39-45, ISSN 2212-8271, https://doi.org/10.1016/j.procir.2017.03.103
[15] Yingfeng Z, Geng Z, Ting Q, Yang L, Ray Y, Analytical target cascading for optimal configuration of cloud manufacturing services, Journal of Cleaner Production, 2017, Volume 151, Pages 330-343, ISSN 0959-6526, https://doi.org/10.1016/j.jclepro.2017.03.027
[16] Yongkui L, Lihui W, Vincent W, Xun X, Lin Z, Scheduling in cloud manufacturing: state-of-the-art and research challenges, International Journal of Production Research, 2019, 57:15-16, 4854-4879, DOI: 10.1080/00207543.2018.1449978
[17] Ellwein C, Riedel O, Meyer O, Schel D, Rent 'n' Produce: a secure cloud manufacturing platform for small and medium enterprises, 2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), 2018, pp. 1-6, doi: 10.1109/ICE.2018.8436332
[18] Zhi L, Vatankhah B, George Q, Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform, Robotics and Computer-Integrated Manufacturing,2018, Volume 54, Pages 133-144, ISSN 0736-5845, https://doi.org/10.1016/j.rcim.2018.05.011
[19] Esposito C, Castiglione A, Martini B, Choo K, Cloud manufacturing: security, privacy, and forensic concerns, IEEE Cloud Computing, 2016, vol. 3, no. 4, pp. 16-22, doi: 10.1109/MCC.2016.79
[20] Yi H, A post-quantum secure communication system for cloud manufacturing safety, J Intell Manuf , 2021, 32, 679–688, https://doi.org/10.1007/s10845-020-01682-y
[21] Anton F, Borangiu T, Răileanu S, Anton S, Ivănescu N, Iacob I, Secure sharing of robot and manufacturing resources in the cloud for research and development, Berns K, Görges D, Advances in Service and Industrial Robotics, RAAD 2019, Advances in Intelligent Systems and Computing, 2019, vol 980, Springer, Cham. https://doi.org/10.1007/978-3-030-19648-6_61

Index

https://doi.org/10.1515/9783110732573-010

This book presents research on the state-of-the-art methods and applications. Security and privacy related issues of cloud are addressed with best practices and approaches for secure cloud computing, such as cloud ontology, blockchain, recommender systems, optimization strategies, data security, intelligent algorithms, defense mechanisms for mitigating DDoS attacks, potential communication algorithms in cloud based IoT, secure cloud solutions.

- Review of cutting-edge technologies and approaches to fill the research gaps in cloud security
- Advanced algorithms for cloud security
- Unconventional approaches for current and future security

THE SERIES: SMART COMPUTING APPLICATIONS

The book series "Smart Computing Applications" provides a platform for researchers, academicians and practitioners to exchange ideas on recent theoretical and applied data science and computing technologies research, with a particular attention to the possible applications of such technologies in the industry, especially in the field of mechanical and industrial engineering.
This series serves as a valuable resource for graduate, postgraduate, doctoral students, researchers, academicians and industry professionals.

www.degruyter.com
ISBN 978-3-11-073750-9
ISSN 2700-6239