Investigations for the improvement of the Cyber Security using Cloud Computing methods and Architecture

Thesis submitted to Srinivas University in partial fulfilment of the Requirements for the award of the Degree of

DOCTOR OF SCIENCE (D. Sc.)

In the Area of Computer Science and Engineering

By

Dr. SAI MANOJ KUDARAVALLI

B.Tech,M.Tech.,Ph.D. (Computer Science & Engineering),C Eng., MIE, MCTS, MCSI

CEO, Innogeecks Technologies & Amrita Sai Institute of Science and Technology, Vijayawada – 520010, INDIA.

SRINIVAS UNIVERSITY

Mukka- 574146, Mangalore, Karnataka State, INDIA

March 2020

This thesis is dedicated to my beloved Parents & Wife

For their endless love, support, encouragement and prayers

Investigations for the improvement of the Cyber Security using Cloud Computing methods and Architecture

Table of Contents

Part II – Publications of the Author

Detailed Table of Contents

CANDIDATE'S DECLARATION

I, **Dr. Sai Manoj Kudaravalli**, declare that this thesis, entitled " **Investigations for the improvement of the Cyber Security using Cloud Computing methods and Architecture",** submitted for the award of the degree of **D.Sc.** of this University, has not been submitted earlier for the award of any degree or diploma of this or any other University.

Date:

Place: Mangalore   Signature of the Candidate

SRINIVAS UNIVERSITY

(Private university established under Karnataka state act No 42 of 2013)

Srinivas Nagar, – 574 146, Mangalore, Phone :0824-2477456, 2425966

Web~~: www.srinivasunniversity.edu.in, ~~Email: info@srinivasuniversity.edu.in

Office of the Director – Research and Innovation council Date:

CERTIFICATE

This is to certify that this thesis entitled “Investigations for the improvement of the Cyber Security using Cloud Computing methods and Architecture” has been submitted by Dr.Sai Manoj Kudaravalli for the award of the degree of D.Sc. of Srinivas University.

Signature of the Director

PREFACE

This basis for this research originally stemmed from my passion for developing better methods of data storage and preservation. As the world moves further into the digital age, generating vast amounts of data and born digital content, there will be a greater need to access legacy materials created with outdated technology. How will we access this content? It is my passion to not only find out, but to develop tools to break down barriers of accessibility for future generations. In truth, I could not have achieved my current level of success without a strong support group. First of all, my parents, who supported me with love and understanding. Secondly, my committee members, each of whom has provided patient advice and guidance throughout the research process. Thank you all for your unwavering support.

ACKNOWLDGEMENTS

I would like to express my thanks to several people and institutions:
First I express my heartiest gratitude to Professor. P.S.Aithal, Vice-Chancellor , Srinivas University for his thorough guidance and enormous help for each and every progression in my D.Sc., work. He has been an inexhaustible source of ideas and always has taken time to discuss patiently every detail of the work. I extend my thanks to Dr.Praveen Dean Research for his constant encouragement. My Deep gratitude to President Srinivas University for providing excellent R&D. facilities on the campus.

Last but not least I want to thank all the colleagues and professors in Innogeecks Technologies & Amrita Sai Institute of Science and Technology for adding value to technical discussions and for pleasant conversations.

My parents, K.Rama Mohana Rao & Bhavani Devi, my wife Gadde Maanasa and my sons (Ayaanshu and Sreeyanshu), my sister Mrudula & my brother Mahesh – without whose love and support this work would have been a dream.

Dr.K.Sai Manoj

ABSTRACT

Recent technological advancements have provided portable computers with wireless interfaces that allow networked communication even when a user is on the move. Although notebook computers and personal digital assistants (PDAs) of today’s first-generation are self-contained, networked mobile computers are part of a larger computing infrastructure. Mobile computing-using a portable device capable of wireless networking-is likely to revolutionize how devices are used. Wireless networking significantly increases the utility of a portable computing unit. It allows smartphone users to connect with other people in a flexible way and to report important events in a timely manner, but with far more versatility than with cell phones or pagers. This also enables uninterrupted access to terrestrial network infrastructure and resources. The convergence of networking and mobility would enable new technologies and facilities, such as interactive tools to facilitate impromptu gatherings, online bulletin boards whose contents are customized to current audiences, lighting and heating to match the needs of those present, and navigation software to guide users in unfamiliar places and on tours. However, the technological obstacles that mobile computing must address in order to reach this capacity are hardly trivial. Many of the problems of software design for mobile computing systems are very different from those involved in software design for today's stationary networked systems. Entire dissertation is based on the concept of a unique research model to identify the gap between ideal system/technology and present system/technology and to identify opportunities to minimize the gap to improve the system/technology towards ideal level. . In this innovative research work introduced Constant Interval Frequency Used Policy that would provide time frame for access link delay connecting the routers and subscribers through this Constant Interval we could have find the attacks. Also investigated on the new Optimization on 5G Software-defined networking (SDN) approach in order to route the requests to the proper Mobile Cloud Computing (MCC) server instance. In this innovative thesis Omnet + + software tool is used to simulate the entire scenario.

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

SaaS	Service as a Service
PaaS	Product as a Service
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
AWS	Amazon Web Services
PDA	Personal Digital Assistant
SDN	Software-defined Networking
MCC	Mobile Cloud Computing
ICT	Information and Communication Technology
NIST	National Institute of Standards and Technology
VM	Virtual Machine
CPU	Central Processing Unit
OSA	Open Security Architecture
CC	Cloud Computing
CSA	Cloud Security Alliance
IETF	Internet Engineering Task Force
SNIA	Storage Networking Industry Association
API	Application Program Interface
MSP	Managed Service Provider
DoS	Denial-of-Service
DDoS	Distributed Denial-of-service
CSP	Cloud Service Provider
SSH	Secure Shell
PCI DSS	Payment Card Industry Data Security Standard
SAS	Statement on Auditing Standards
FAT	File Allocation Table
NTFS	New Technology File System
IDT	Interrupt Descriptor Table
SAML	Security Assertion Mark-up Language
SP	Service Provider
IDP	Identity Provider
SSL	Secure Sockets Layer

TLS	Transport Layer Security
TCP	Transport Control Protocol
IP	Internet Protocol
SSO	Single Sign-on
NaaS	Network as a Service
PBE	Predicate Based Encryption
ABAC	Attribute Based Access Control
PDFSP	Partially Distributed File System with Parity
HDFS	Hadoop Distributed File System
GFS	Google File System
IBC	ID-Based Cryptography
PET	Privacy Enhancing Technologies
PBE	Predicate Based Encryption
UCDDES	Uncrackable Cipher Dynamic Double Encryption Standard
DTN	Delay Tolerant Network
AMV	Adaptive Mobile Video Streaming
ESV	Efficient Social Video
DACSDC	Data Access Control and Secure Data Confidentiality
ACDC	Access Control and Data Confidentiality
BS	Base Station
GMM	Group Mobility Model
CDM	Cache Decision Model
CR	Content Router
AP	Access Point
PEKS	Public Key Encryption Search
TCG	Trusted Computing Group
SL	Spatial Locality
TL	Temporal Locality
DLR	Dual Locality Ratio

Chapter 1

1 Chapter 1 : Introduction to Caching Method of Server Design

1.1 Introduction to Caching Method of Server Design

The main problem in caching is content caching and task caching; therefore, based on the caching method server should assign it. Still Cloud with server setup not able to catch and store all types of computation storage. Usually, the Collaborative resource allocation method defined in the caching technique with three classification Voice User, data User, and Offloading user. Regular user adopts with spectrum utilization, and data user generates utility due to spectrum and cache. The offloading user creates Service due to the spectrum and computational resources. Every Base Station connected with Mobile Cloud Computing Server for Computational task offloading and which is not consider the virtualization with interference in Neighbour Cloud to handle Interference issue

In the processing of data offloading in multiple users and multiple servers, Mobile Cloud computing tasks can be processed on Cloud or locally in a 5G Cellular network. Though, when the 5G cellular task cached in the Cloud, it may not need to be processed locally in the advanced network. Based on the deciding task, how many tasks to offloading is a challenging issue. After that, it is challenging to make a task offloading in data with task caching using an advanced network.

Mobile Cloud Computing Optimization problem in 5G cellular network: When computing and storage resources at Cloud are limited, giving task caching and offloading problems and solving this problem is a challenging issue. It is because Mobile Energy Cloud computing multiple energy task caching and offloading scheme needs careful coordination

Mobile Cloud Computing is developing in recent years, which provides this computation without delay and high performance by deploying Cloud servers in the mobile network. The Cloud servers compute the user requirement within a fraction of second, and it is very suitable for delay-sensitive tasks. Decrease the delay and energy used for computation, the mobile Cloud computing requires two essential aspects, and they are Cloud Caching and task Offloading.

Cloud caching application data revealed and easy to access through unauthorized ones. Cloud Cache data's has a threat from hackers and leaking information

1.1.1 Cloud Caching:

Cloud Caching is also known as content offloading. The Modern world variety of technologies available to improve the application and user application response. Reduce the delay and energy, the vital content cached in the Cloud. The server uses the content from the cache to reduce the time and energy required to get details from the device.

1.1.2 Task offloading:

This vital task in mobile Cloud computing. When and where the task needs to be offloaded from the user device to the mobile Cloud to save energy and time is called task offloading. The main problem in Mobile Cloud computing is the storage capacity of the Cloud. The storage capacity of the Cloud is very less. But the computation and the storage capacity should be significant comparatively to perform the task offloading. In practical, the hardware and software resources to perform the computation and storage is lesser than the assumption.

1.2 Introduction:

This chapter pointed on the Research Objectives, goals, and Research outcomes of this dissertation. The main focus is on the implementation of the cybersecurity methods related to cloud computing

This innovative research is also strictly concentrated on the new security and privacy challenges, especially on the problem by mobile cloud computing servers. It also concluded the contributions in addressing these challenges.

1.2.1 Fundamental Concepts:

Modern days, many people connected with the digital era by sharing communication in so many ways using information and communication technology (ICT). The key factor involved in this simple way of accessing from any point of location. The radical and pervasive change in information technology such as the

Internet playing the leading role for various groups such as research scholars, business applications, researchers, students, professors, professionals, etc. to complete their assignments with so many ways to achieve their targets. Many developers associate with the Internet and hold the IT infrastructure to fulfill their tasks as per their technical requirements. Nowadays, technical experts have a lot of necessity of internet usage; the services provided such as Data, Storage, Platform, Software, Infrastructure services, etc. through the Internet also rapidly increased. Modern-day cloud computing technology is developing with so many services with a vast number of persons via an extensive area network. Persons can get maximum benefits using cloud services on a payment basis to the cloud service provider with less cost.

Because of the critical status or nature of their applications, it possible for the vital role that the cloud environment is secure. The primary purpose of security challenges with clouds is that the authenticated owner of the data may not have control of different sectors where the data placed. One must also utilize the various resource memory allocations and scheduling processes provided by cloud platforms if one wants to exploit the benefits of using cloud computing. Therefore, we need to safeguard the data in the middle part of the untrusted processes [1].

Cloud computing is very much popular day by day. The reason behind many of the IT companies has a requirement to store their information. The general definition of cloud computing provided by the National Institute of Standards and Technology (NIST).In another case, it is generally a paradigm that provides required computing resources and storage. In contrast, for others, it is just a way to access software and data operations from cloud computing. Now everywhere widely used in Cloud computing, it is popular in the organization, scientific, research and academic, defence today because cloud environment provides its users readability scalability, integrity, reliability, flexibility, and availability of data.

Cloud computing also provides minimal cost by enabling the required sharing of data to the organization/ host industries. Organization or industries can import their data into the cloud so that their shareholders or authenticated user can utilize their data. Apple's apps or Google apps is best as an example of cloud computing operation structures.

However, Cloud computing provides different facilities and benefits, but still, it has arisen a few issues regarding safety access and ample storage of data. In this thesis, we analyse the security issues related to the cloud computing model and its services, applications [3].

1.2.2 Cloud computing characteristics:

On-Demand self-service: A cloud might be an individually attain use computing possibilities, as per the use of various servers, network storing, as on request, without user communicating with the cloud provider.

Broad Network Access: Common services delivered across the Internet within a standard mechanism structure, and access to the services is possible through assorted customer tools.

Resource pooling: A multitudinous model is employed to serve various types of users or clients by making possible pools of different computing resources. As per the request of users, these have various existing resources that can be assigned and reassigned dynamically using authenticate ownership.

Rapid Elasticity: Capabilities might be elastically provisioned or rapidly released. From customers o user view, the Service provided possibilities come out to be within limitless and must have the user or customer capability to purchase or sell in any quantity at any time.

Measured Services: The provision operation procured by various clients is measurable—the use of assets calculated through directed, estimated and accused of contributor and asset.

1.3 Background

The below descriptions are the express background of learning concepts efficiently.

1.3.1 Cloud computing:

Cloud computing is rapidly or continuously developing as a standard for sharing and service the data over the remote storage areas in an online cloud server environment.

1.3.2 Authentication:

An authenticated user or customer can access its data item fields. The legal user can identify only the authorized partial or entire data fields through login operations, and any forged or tampered data fields cannot be directed by the deceive the valid user or customer.

1.3.3 Cloud storage:

Cloud storage means the storage of massive amounts of data online in the cloud environment, wherein a company or organization's data stored in and accessible from multiple possibly distributed operations and connected exiting resources that comprise cloud computing.

1.3.4 Data anonymity:

Any irrelevant small entity cannot recognize the exchanged data and communication state between even it intercepts the exchanged data messages through an open-source channel.

1.3.5 Forward security:

Any adversary cannot correlate or associate two or more communication sessions with deriving the prior interrogations according to the currently continuous captured messages.

1.3.6 User/Client Privacy:

Any relevant or irrelevant entity cannot know or guess a user's or a client's access desire, representing a client's interest in another client's authorized data fields. If and only if either clients or users have mutual benefits to transfer in each other's authorized valid data fields, the cloud computing services will communicate the two or more clients to realize the valid access permission through sharing operations.

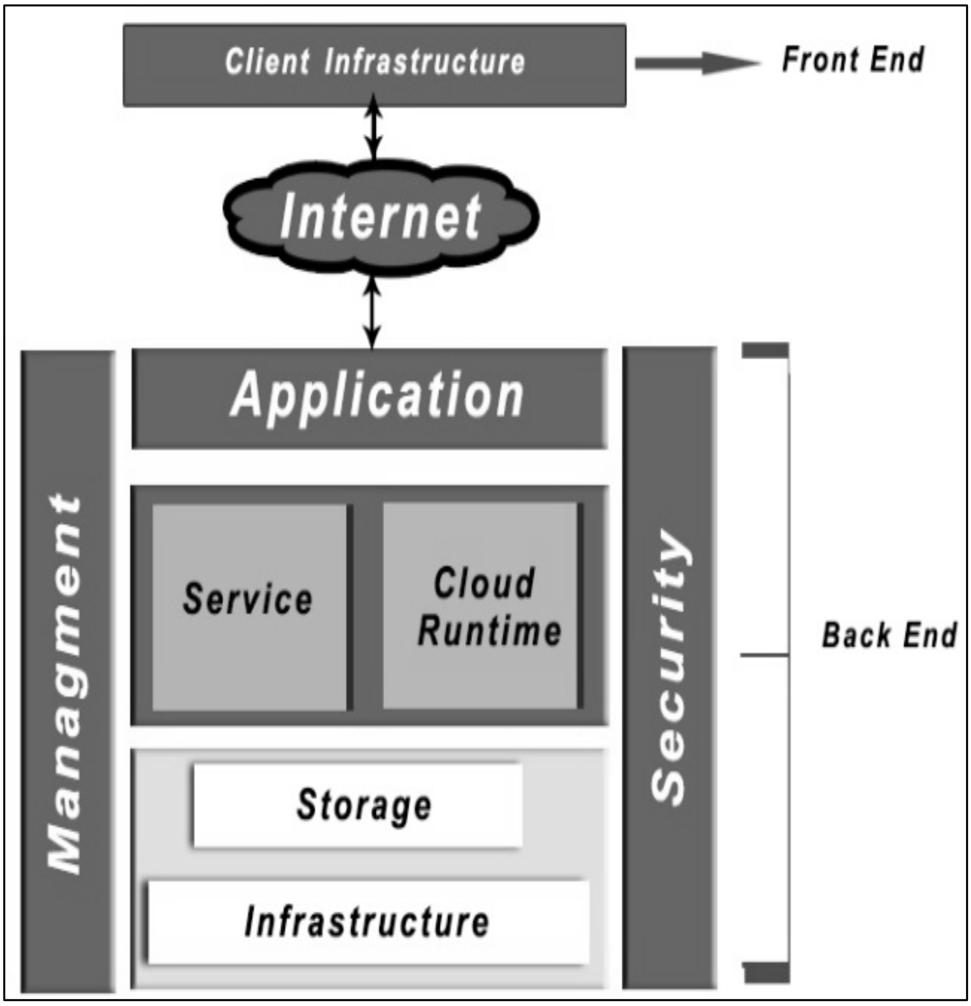


Figure 1:1 Cloud Computing Overview

Cloud Computing concepts:

Weiss, A., 2007. Computing in the Clouds. netWorker Magazine - Cloud computing: PC functions move onto the web, (Volume II, Issue 4), 16–25.

Based on the concept cloud computing analysed as a computing style with scalable computing capabilities that can be delivered 'as a service' to users using Internet technologies (Weiss 2007, Mell and Grance 2009, Vaquero et al. 2009). In current technology development, users can quickly gain access to applications or take full advantage of their resources in the Cloud at a small cost.

Mell, P., and Grance, T., 2009. The NIST Definition of Cloud Computing. National Institute of Standards and Technology, 53 (6).

According to the NIST, cloud computing has five main characteristics (Mell and Grance 2009).

1. On-demand Service – users should receive the intended computing services from their service providers. 2. Broad Network Access – the Service should be available for access through the network using any type of devices, such as tablets, laptops, and computers. 3. Resource Pooling – Cloud resources are pooled and used by different users concurrently (multi-tenancy); the user might choose the location or region for his machines but without being aware of their exact location. 4. Rapid Elasticity – users should be able to acquire suitable computing capabilities. Users may automatically increase and decrease the resources used. 5. Measured Service – users pay only for what they use.

In cloud computing, there are three recognized service models: software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS) (Mell and Grance 2009, Weinhardt et al. 2009, Ertaul et al. 2010). These explained below.

1. SaaS model – service providers, offer their applications to users through the network. Users can access the applications using thin clients and browsers or program interfaces designed to communicate with the other applications hosted in the Cloud.

2. PaaS model is mainly offered for application developers as a development environment to host and support developers with libraries, services, tools, networks, and storage.

3. IaaS model – provides the infrastructure and resources to host users' machines (virtual machines). IaaS providers offer computing power, storage, networks, and any other supporting resources to host virtual machines (VMs). Each host in the Cloud IaaS model is occupied by several VMs sharing the resources; the VMs are isolated by the virtualization layer.

Milenkoski, A., Iosup, A., Kounev, S., Sachs, K., Ding, J., and Rosenberg, F., 2013. Cloud Usage Patterns : A Formalism for Description of Cloud Usage Scenarios. Tech Report SPEC-RG-2013-001 v1.0.1, SPEC Research Group, 12–13.

IaaS, PaaS, and SaaS signify an abstract level, with IaaS being the lowest abstraction level. IaaS may provide services to PaaS and SaaS, PaaS may provide services to

SaaS but not to IaaS, and SaaS may not provide services to PaaS or IaaS (Milenkoski et al. 2013).

1.4 Cloud Storage Highlights:

1.4.1 Rouse, M., 2005. What is storage? [online]. TechTarget. Available from: http://searchstorage.techtarget.com/definition/storage [Accessed 12 Mar 2015].

Computer storage is where data held. Storage has divided into primary storage, which contains data in memory (RAM) and other "built-in" devices such as the processor's L1 cache and secondary storage, which stores data on hard disks and other devices requiring input/output operations (Rouse 2005). Primary storage provides faster access than secondary storage, mainly because of its close location to the processor or the architecture of the storage devices. On the other hand, secondary storage can store more data than primary storage, and this includes external hard disks and USB flash drives (Rouse 2005).

1.4.2 Wu, J., Ping, L., Ge, X., Ya, W., and Fu, J., 2010. Cloud storage as the Infrastructure of Cloud Computing. In: Proceedings - 2010 International Conference on Intelligent Computing and Cognitive Informatics, ICICCI 2010. 380–383.

Cloud storage is known as utility storage if delivered through public cloud service providers (Wu et al. 2010). On the other hand, private service providers offer the same scalability, flexibility, and storage mechanism with restrictions or non-public access. Cloud storage runs on a virtualization platform providing end users and applications with a scalable and provisioned virtual storage architecture. Generally, cloud storage accessed through an API (Wu et al. 2010, Ju et al. 2011).

Cloud storage defined as a cloud computing model that stores data on distributed servers and is accessible anywhere through the Internet. A cloud service provider maintains, operates, and manages storage servers built using virtualization techniques (Wu et al. 2010).

1.5 CLOUD COMPUTING SECURITY ARCHITECTURE:

Cloud Security within surrounding cloud computing is mainly worried about a few security issues because the personal devices used to provide necessary services do not belong to the users or clients themselves. The users have no control of their operations, or any amount of knowledge, what could happen to their data sharing. It is a reasonable effort concern when clients have valuable and personal authenticated information stored in a cloud computing storage and retrieval service. Users or clients will not compromise their privacy needs, so cloud computing service providers are must ensure that the customer's or clients' information is a safe manner.

However, challenging various factors because as security levels developments are made in different areas, there always seems to be a particular thing that identifies to figure out a possible way to disable the security and taken advantage of user information to store a secure place. The minimal essential components of Service Provider Layer are SLA Monitor, Metering operations, Accounting, Time Scheduling, Resource Provisioning, Scheduler& Dispatcher, Load Balancer, Advance Resource Reservation Monitor, Data traffic controller, retrieval process analyzer and Policy Management [3]. Some of the security issues related to Service Provider Layer are Identity, Infrastructure, Privacy, Data transmission, People and Identity, Audit and Compliance, Cloud integrity, reliability, association ship, and Binding Issues.

Some of the essential components or things of Virtual Machine Layer create many virtual machines and several external operating systems and its monitoring all operations. Some of the security issues are arises related to Virtual Machine Layer are VM Sprawl, VM Escape, Infrastructure, data load failure, Separation between Customers, Cloud security legal and Regularity issues, Identity and Access management operations. Some of the essential components or things of Data Center (Infrastructure) Layer contain the IaaS Servers, CPU's, memory management, and storage. Henceforth is typically hypothetically denoted as Infrastructure-as-a-Service (IaaS).

Another case security issues related to Data Centre Layer are secure data at rest, and Physical Security combined with the Network and Server revival process. Few organizations have been mainly focusing on security leaks and issues in the cloud environment. The Cloud Security Alliance is a non-profit organization that creates and promotes the use of best possible practices for providing security assurance within Cloud Computing and provides research, organizations, education on the applications of Cloud Computing in the aspect of security based on the computing platforms [4]. Cloud computing - Open Security Architecture (CC-OSA) is another organization focusing on security issues and risk management.

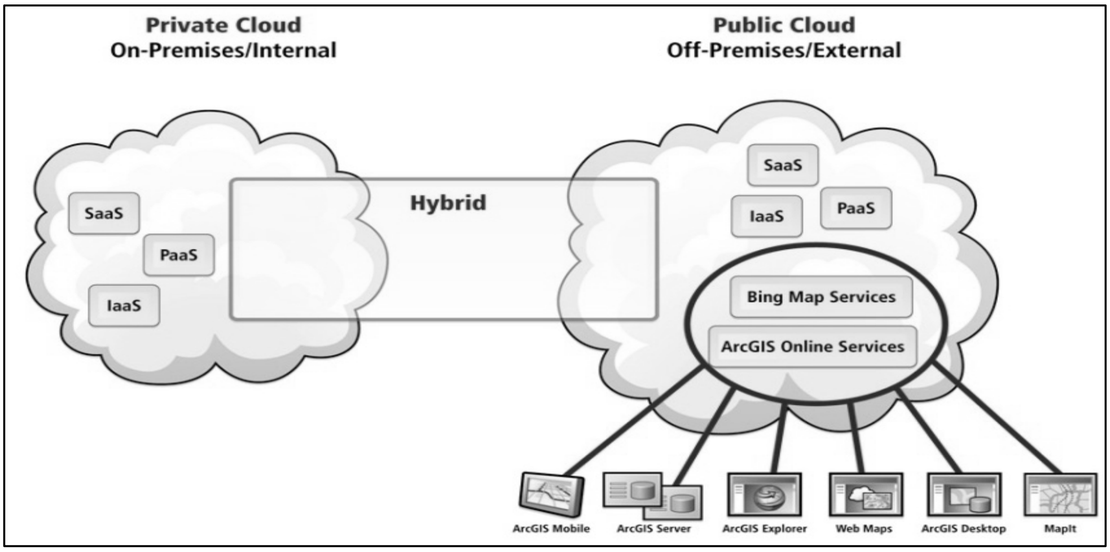


Figure 1:2 Cloud computing mapping retrieval process

They propose the OSA pattern, possible design attempt to illustrate core cloud functions and operations, the critical roles for oversight and risk mitigation, collaboration across various internal organizations through on-demand basis, and the controls all operations that require an additional emphasis basis. For example, the security Certification, Accreditation, and Security Assessments series increase in a vital role to ensure oversight operations and quality service. The assurance is that the operations are being "outsourced operations" to another service provider [5]. System and Services Acquisition is crucial and critical to ensure that acquisition of quality services is managed reliability manner. Contingency planning stages help to ensure a close understanding possibility of how to respond in the event of interruptions in the existing environment to quality service delivery.

The Risk Assessment controls play critical roles in understanding the risks and threats associated with services in a business or marginal context. National Institute of Standard and Technology (NIST), USA, has initiated and maintains standards, and quality activities to promote standards for cloud computing and alliance branches. To maintain address the risk challenges and enable cloud computing operations, several standards groups and industry research consortia develop on related specifications and testbeds.

Some of the existing standards support and test alliance groups are Cloud Security Alliance (CSA), Internet Engineering Task Force (IETF), and Storage

Networking Industry Association (SNIA), etc. On the other side, cloud APIs provide either a functional requirement interface or a management interface. Cloud security management has multiple aspects that can be standardized multiple channels for interoperability. Some of the possible standards are Federated security such as identity across clouds, numerous data sets, Metadata and data exchanges among clouds, Standardized outputs for monitoring, auditing, billing, reports and notification for cloud applications and security services, Cloud-independent representation for risk policies and governance, etc., below Figure showing the high-level view of the cloud computing security architecture [6].

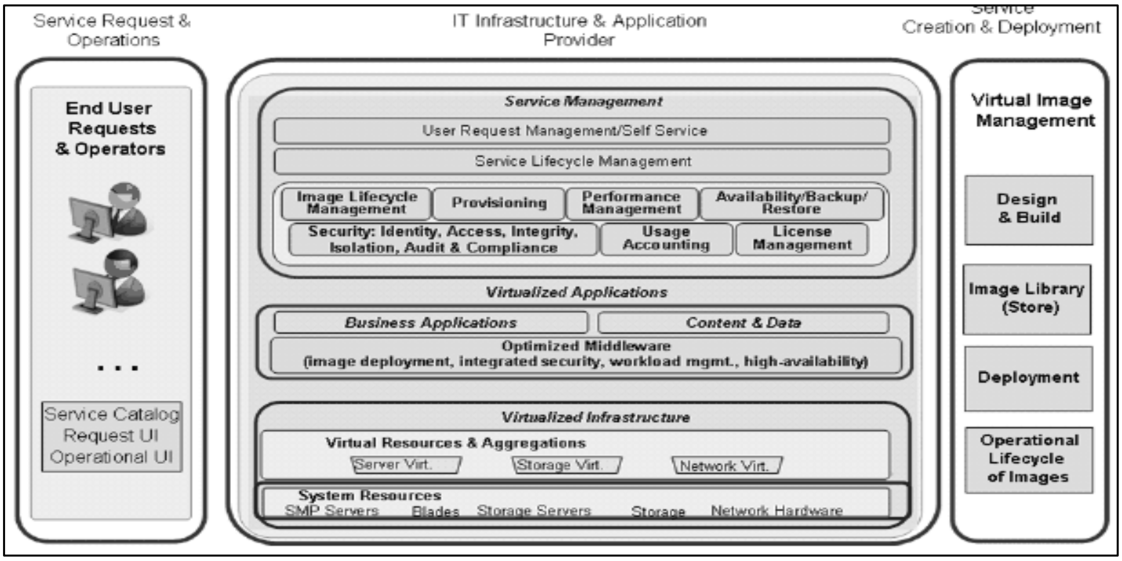

Service Request & Operations
IT Infrastructure & Application Provider
Service Creation & Deployment
End User Requests & Operators
...
Service Catalog
Request UI
Operational UI
Service Management
User Request Management/Self Service
Service Lifecycle Management
Image Lifecycle Management
Provisioning
Performance Management
Availability/Backup/ Restore
Security: Identity, Access, Integrity, Isolation, Audit & Compliance
Usage Accounting
License Management
Virtualized Applications
Business Applications
Content & Data
Optimized Middleware
(image deployment, integrated security, workload mgmt., high-availability)
Virtualized Infrastructure
Virtual Resources & Aggregations
Server Virt.
Storage Virt.
Network Virt.
System Resources
SMP Servers
Blades
Storage Servers
Storage
Network Hardware
Virtual Image Management
Design & Build
Image Library (Store)
Deployment
Operational Lifecycle of Images

Figure 1:3 Cloud computing security architecture

1.5.1 About Cloud Computing Architecture real-time concepts:

The existing cloud computing architectures differ in many ways. Security has been a severe issue as client-related data and processing the infrastructure provided by third-party service providers vary greatly. It is necessary to know the extent of security inclusion into the cloud computing system and then find the best architecture that includes the best and sophisticated security system.

In this research work, a comparison of existing architectures from the perspective of inclusion of security infrastructure within the cloud computing system presented along with an overall architecture included with every aspect of security, taking into account the most of the vulnerabilities.

The vast number of components considered into a cloud computing system architecture, essentially explains how the components are structured and how the communication happens among the elements. The ingredients found and placed in the architecture include cloud resources, services, middleware, application, and system software. Nothing about the hardware, as such, is described in architecture. The architecture explains the properties of the software objects and the relationships between the objects.

Architecture points out the cloud computing infrastructure deal with various aspects include Xaas Structures, platform adaption, structuring cloud services, structuring cloud components, the relationship between different components, especially when related to exporting data across the continents[4].

Many components exist within the cloud infrastructure. Data storage and retrieval are made available as a service to the user. When it comes to the data, confidentially of the same is essential. Every component has an architecture built into overall cloud computing architecture. Many storage devices that either supported on the servers or the network storage devices clustered to form the total storage. Dedicated software running on one of the servers is made responsible for managing the storage in terms of allocation, storing the user data, and retrieving the data as per user requirements. The software also deals with providing access rights to the user for availing the data services and revoking the same when the Service completed.

Security has been the most important issue when it comes to data storage and retrieval and transmitted to the end-user over the Internet. Security was also the issue when the Data transfer from the user to the Cloud implemented.

Cloud storage is not just the data supported on a server as in a conventional system. Cloud storage, as such, includes network devices, storage devices, servers, applications, public access interface, client programs, and similar such systems. A sub-system implemented that manages the storage in the cloud computing environment

Clustered storage architecture generally implemented to provide efficient storage services and support scalability and fault-tolerant data storage and retrieval systems. The cloud storage resources typically organized as a cluster, a grid, or a distributed file system. The connecting network and the storage management software together provide the data storage services to the end-users.

Providing the user the easy access and high-performance data services are the main objectives of cloud computing systems when it comes to data storage and retrieval. The storage infrastructure provided in cloud computing systems is homogenous and supported on homogenous platforms, while that is not the case now. A heterogeneous cloud storage infrastructure management has been presented [5]

Architecture has presented that considers the management of the requirements by SLAs. Architecture has been proposed based on market-driven policies and virtualization technologies, which supports providing a flexible allocation of services [6].

Virtualized services that are dynamically scalable provided to the users through a service model supported by cloud computing technologies. No standard, as such, exists as on date for implementing cloud computing solutions. Much architecture used for building cloud computing systems. The users' requirements are to be found first and then classify the same based on some criteria. It has shown that some features required by the users, such as the requirements for storage, software, platform, securing the data, etc., play a vital role in defining the architectures that can use to build cloud computing infrastructure [7].

1.5.2 Innovative Investigation on the cloud computing architectures in various models and techniques

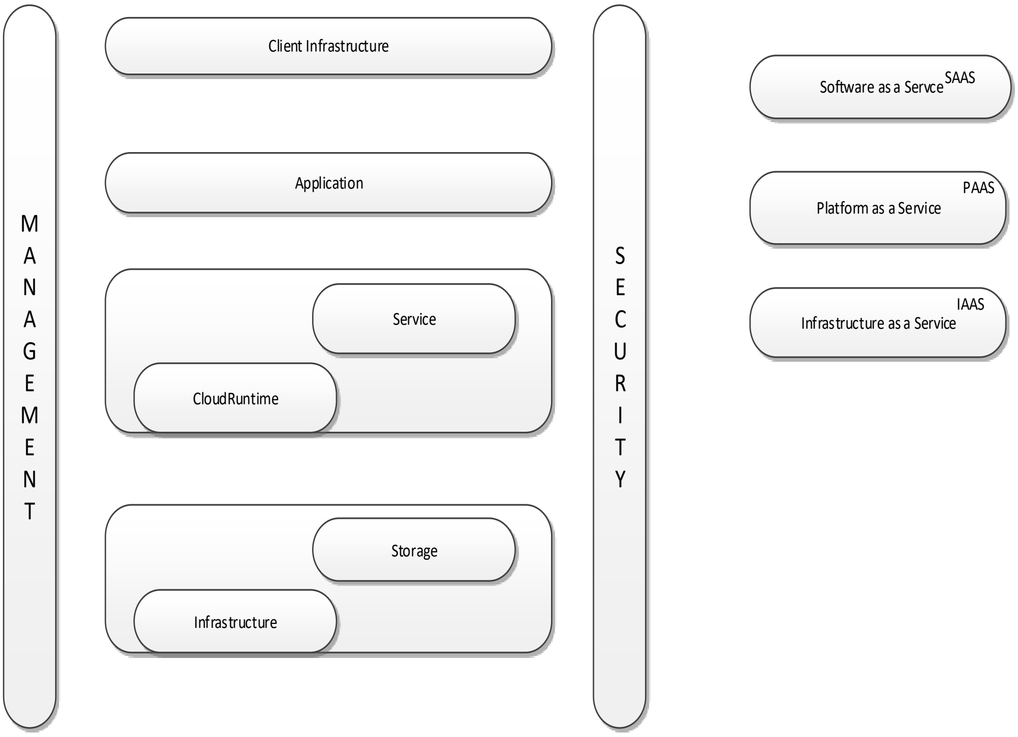


Figure 1:4 Model 1

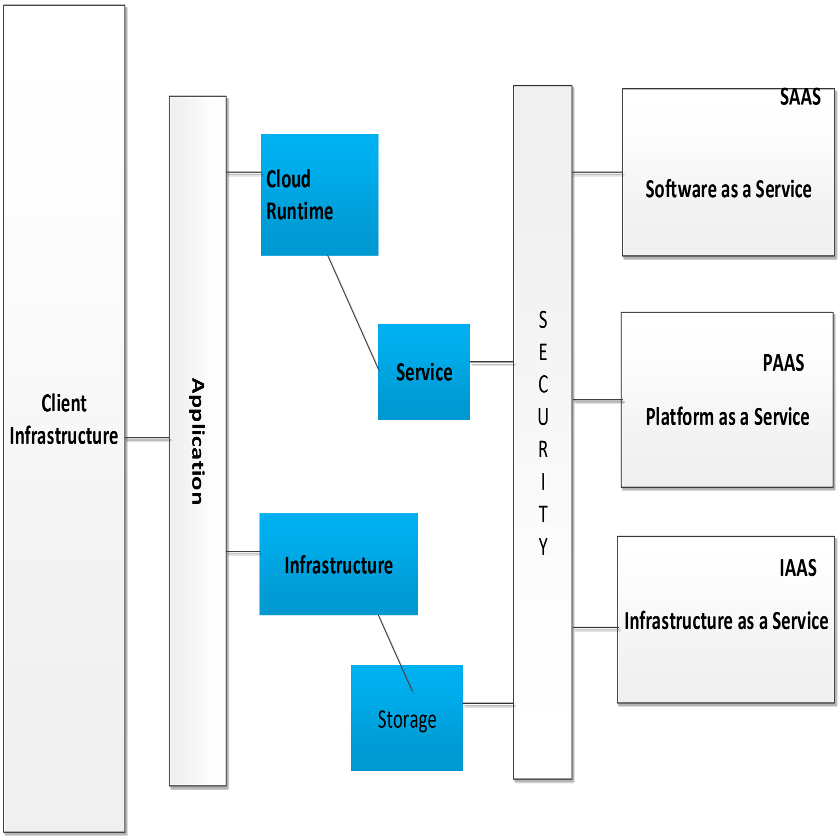


Figure 1:5 Model 2

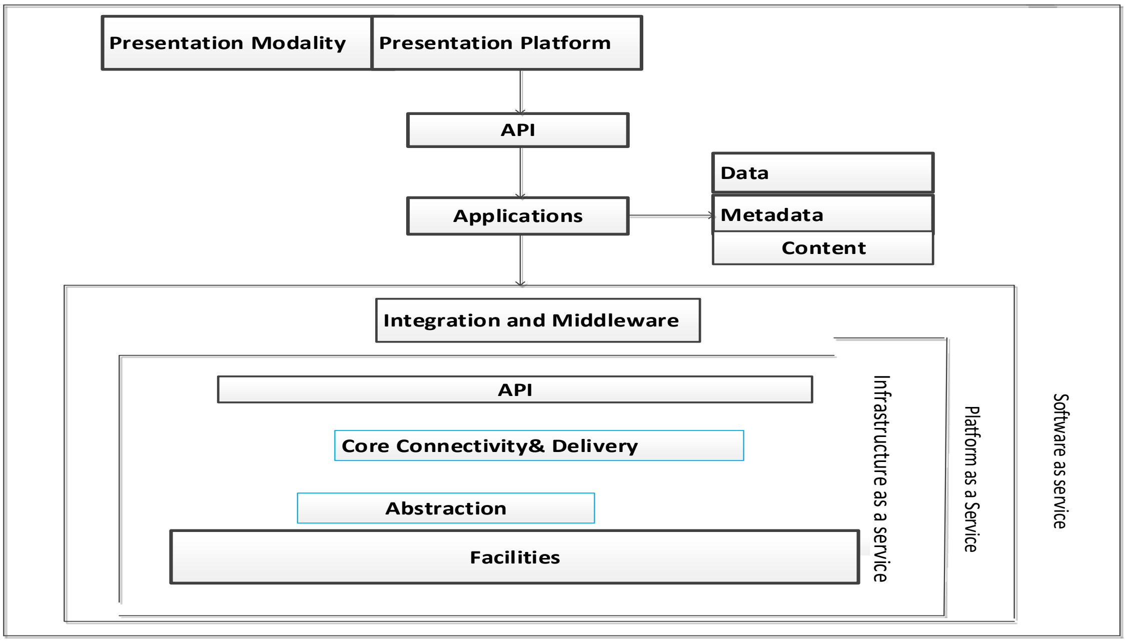


Figure 1:6 Model 3

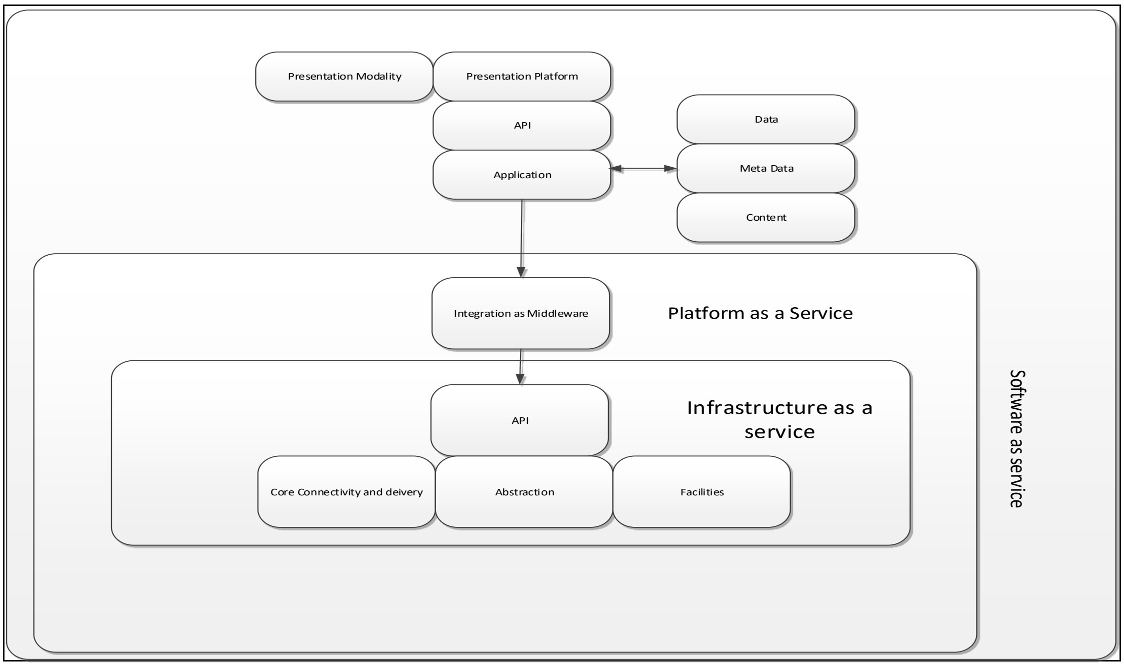


Figure 1:7 Model 4

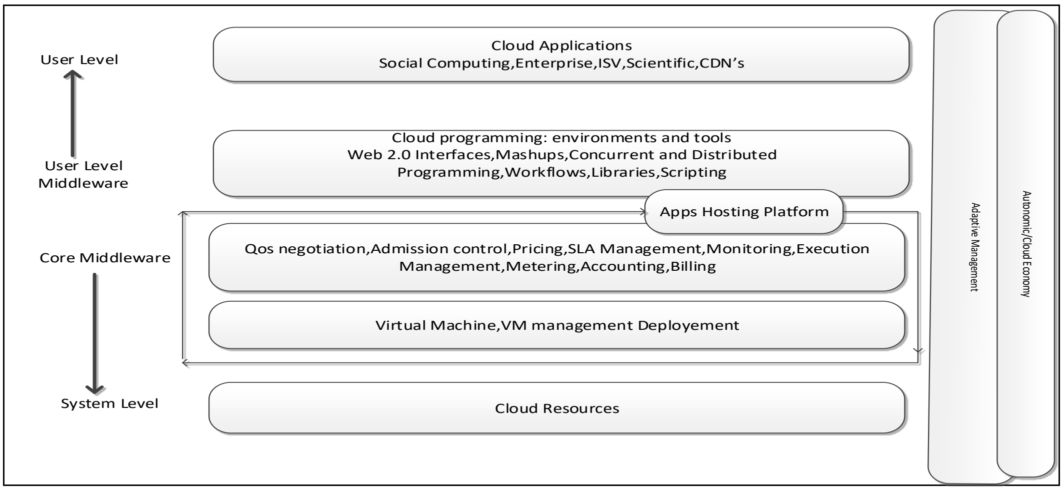

User Level
User Level Middleware
Core Middleware
System Level
Cloud Applications
Social Computing,Enterprise,ISV,Scientific,CDN's
Cloud programming: environments and tools
Web 2.0 Interfaces,Mashups,Concurrent and Distributed Programming,Workflows,Libraries,Scripting
Apps Hosting Platform
Qos negotiation,Admission control,Pricing,SLA Management,Monitoring,Execution Management,Metering,Accounting,Billing
Virtual Machine,VM management Deployement
Cloud Resources
Adaptive Management
Autonomic/Cloud Economy

Figure 1:8 Model 5

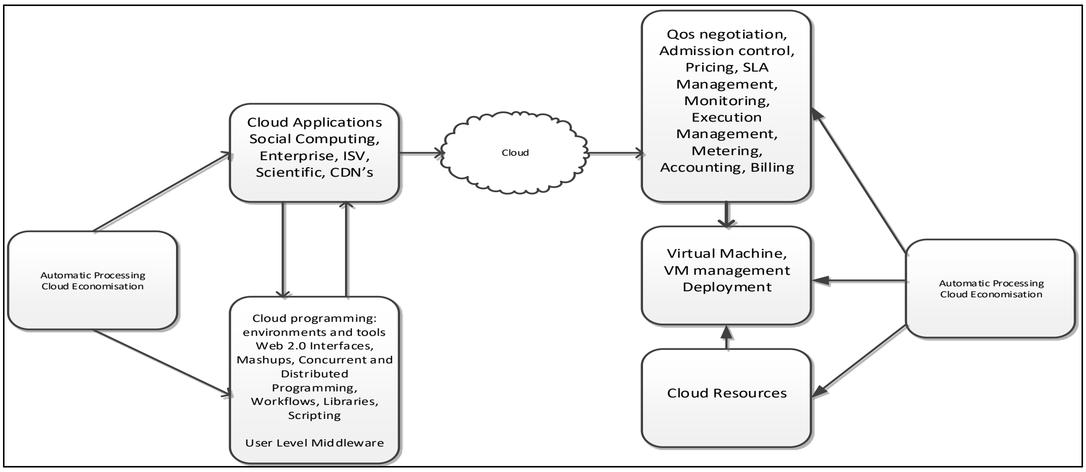


Figure 1:9 Model 6

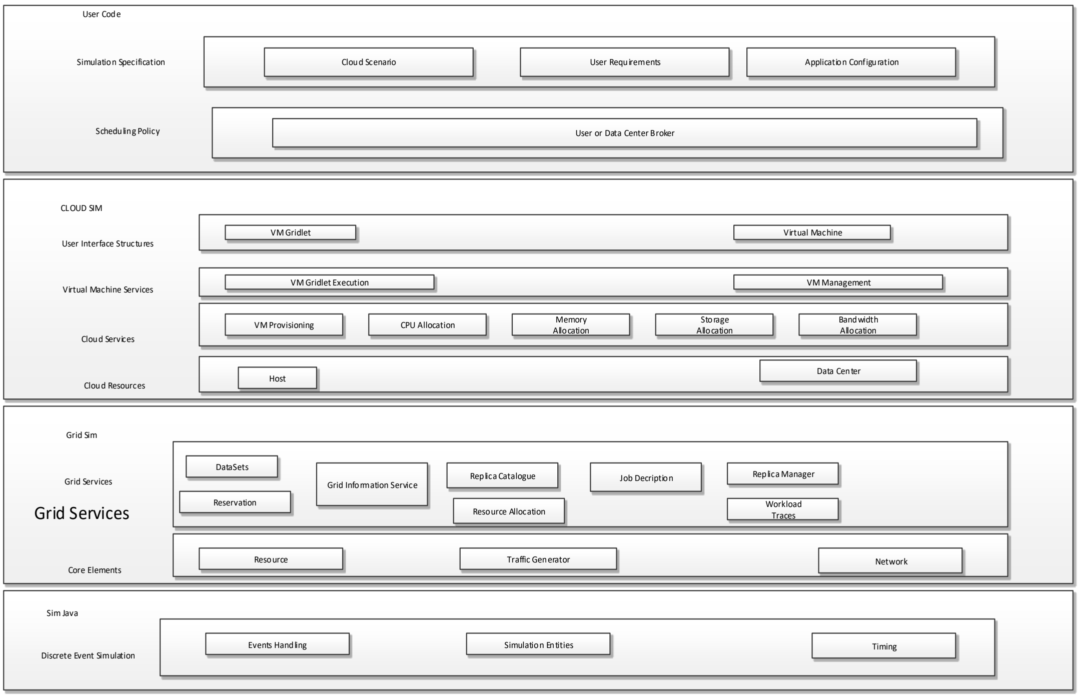


Figure 1:10 Model 7

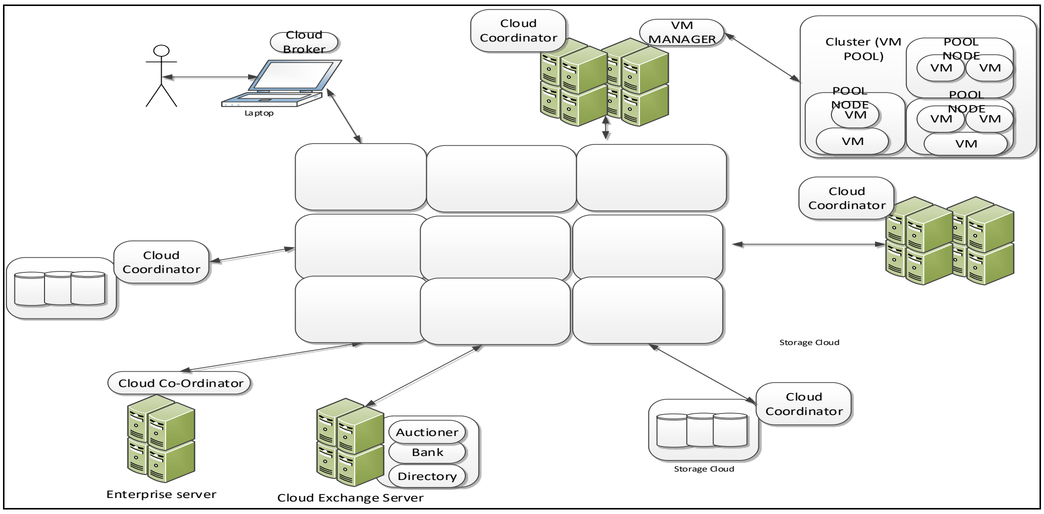


Figure 1:11 Model 8

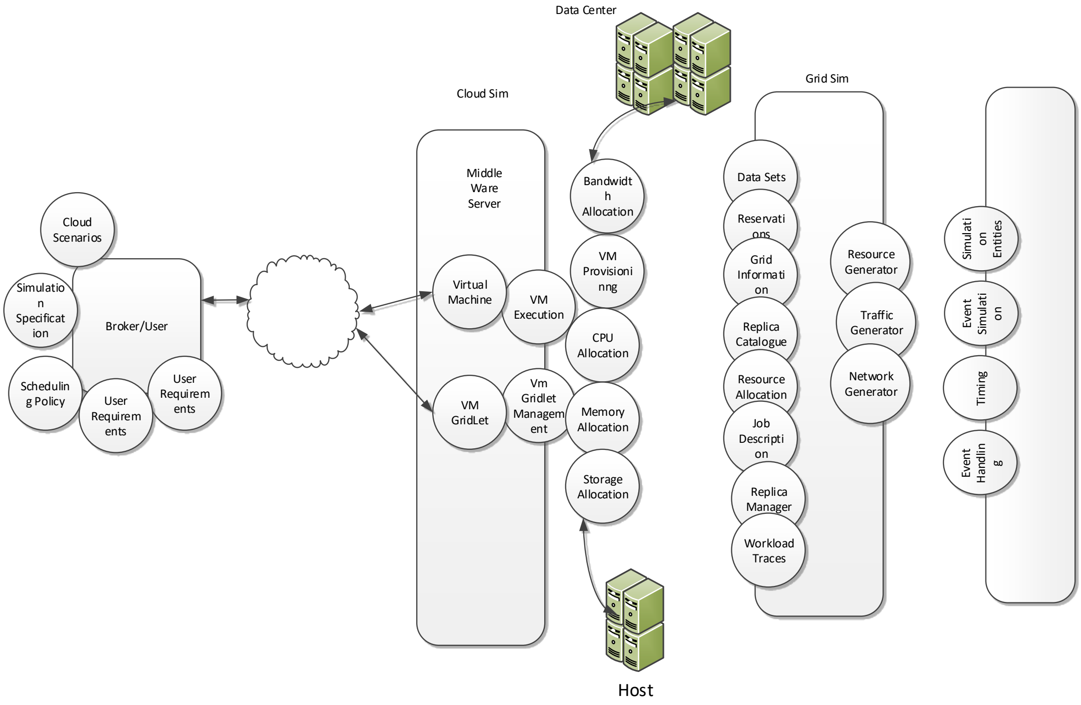


Figure 1:12 Model 9

1.6 KEY SECURITY ISSUES IN CLOUD COMPUTING:

Cloud computing consists of various applications, platforms and infrastructure segments. Each and every segment performs various operations and offers different software products for businesses and individuals around the technical world. The business cloud application includes Software as a Service (SaaS), Utility Computing, Web Services, Platform as a Service (PaaS), Managed Service Providers (MSP), Service Commerce and Internet Integration and Internet service providers channels. There are numerous security and risk issues for cloud computing as it encompasses many relevant technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, server traffic controls, concurrency control and memory management operations [8].

Security issues for many kind of these systems and technologies are applicable to cloud computing. For example, the network combines that interconnects between the systems in a public or private cloud has to be secure and mapping possibilities the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate security policies are enforced for data sharing and retrieval process. The following below operations are the various security concerns in a cloud computing environment.

- Access to Servers & Applications
- Data Transmission
- Virtual Machine Security
- Network Security
- Data Security
- Data Privacy
- Data Integrity
- Data Location
- Data Availability
- Data Segregation
- Security Policy and Compliance
- Patch management

1.6.1 CLOUD SECURITY ISSUES

Organization or companies are uses various cloud services such as IaaS, PaaS, SaaS and the models like public, private, hybrid. These models and services has different cloud security issues. Each service model is associated with some security issues. Security issues are considered in two or more views, first in the view of service provider who insures that cloud services provided by them should be secure and also manages the customer's or users identity management. Other view is client or customer view that ensures that security services that they are using is secure path enough.

1.6.2 Multi-tenancy

A cloud based model is built for various reasons such as sharing of resources, memory management, retrieval processing, storage and shared computing. Multi-tenancy security provides efficient service utilization of resources, keeping cost lower level. It implies sharing of all computational resources, services storage and cloud applications with other tenants residing on the same logical/physical platforms at provider's premises. Thus it violates the confidentiality of data and results in leakage of information and encryption and increases the possibility of attacks, and reduces the security leaks.

1.6.3 Elasticity

It defines the degree to which a system is able to adapt to the data workload changes by provisioning and deranged existing resources in an autonomic possible manner, such that the available resources matches the current on-demand at any time as closely to as possible too share surrounding resources. Elasticity generally implies scalability, integrity and reliability. It replies that consumers or valid users are able to scale up and down as requirement needed. This scaling enables tenants to use a existing resource that is assigned previously to other equal tenant. In this may lead to confidentiality and risk issues.

1.6.4 Insider attacks

Private Cloud model is a multitenant based objective model that is under the service provider's single management operation domain. This is a view on threat that arises within surrounding the organization. There are no limited hiring standards and providers for cloud employees solve these issues. So a third party vendor can be easily hacking the data of one company or organization and may corrupted or sell that data to any other organization.

1.6.5 Outsider attacks

It is the one of the major attack concerning problem issue in an organization or company because it releases the confidential or secrete information of an organization in open access. Clouds in computing, their not like a private network area, they have more Application Process interfaces than private network. So hackers and attackers have advantage of exploiting the API, weakness and may do a connection breaking and easily hacking information from various sources. These attacks are less or minimum harmful than the insider attacks because in the later we sometimes unable to identify the security attack.

1.6.6 Data Loss

As in any cloud, there are multiple mode tenants, data integrity and safety could not be provided. Data loss can results in financial stage, customer or client count loss for an organization. An important example of this can be updating and deletion of any data without having any backup of that data.

1.6.7 Network security

Man in middle attack: - In this attack, an attacker makes an independent connection and communicates between the cloud user on its private network where all control is in the hand of attacker.

Distributed denial of service attacks: - In DDOS attack, servers and networks are brought down by a vast amount of network traffic and clients or users are denied the access to a certain Internet based Service operations.

Port scanning: - Port is a place from where information exchange takes place and identifying object verifies virtually. Port scanning is taking place when subscriber configures the group. Port scanning is done automatically when you configure the internet so this violates the security reason concerns.

1.6.8 Malware Injection Attack Problems

In cloud computing, a vast of data is transferred between cloud service provider and valid client or consumer, there is a need of customer authentication and authorization. When the original data is transferred between cloud service provider and user, attacker can introduce interrupt or malicious code into it. As a possible result, the original valid user may have to wait until the completion of the job that was maliciously introduced.

1.6.9 Flooding Attack Problem

In cloud computing, there is a no. of qualitative servers that communicate with one another and transfer data. The possible requests is processed, the requested jobs are authenticated initially, but this authentication process requires a vast amount of CPU utilization, memory allocation and finally due to these server side is overloaded [8] and it passes request its offload to other server. By all this the as usual processing of system is interrupted, and the system is flooded automatically.

1.7 PROPOSED SYSTEM

We are conducting survey and research on secure cloud computing in different factors. Due to the extensive complexity cases of the cloud, we observed contend that it will be difficult to provide a holistic solution to securing problem in the cloud, at present technology strategies. Therefore, our possible goal is to make increment in order enhancements to securing the cloud that will ultimately give result in a secure cloud. In particular case, we are developing a secure cloud environment consisting of hardware (includes 1024TB of data storage on a mechanical non-volatile disk drive, 2400 GB of memory and multiple commodity computers), software (includes Hadoop) and data (a semantic web data repository).

Our cloud system will:

a) Support efficient cloud storage of encrypted sensitive data,
b) Store, manage and query massive amounts of data,
c) Support fine-grained access control
d) Support strong authentication and validation.

In this thesis, we describe our normal approach to securing environment the cloud. The organization of this paper is as follows: we will give an overview of security issues for cloud storage. We will discuss secure third party authentication of data in clouds. We will discuss how encrypted data may be queried in procedural manner and discuss Hadoop for cloud computing operations and our approach to secure query processes with Hadoop map reducing.

In this research work, we are focusing on some aspects of the secure cloud storage, namely known aspects of the cloud storage and data layers. In particular,

We describe various ways of efficiently storing objects on the data in foreign machines,

Querying encrypted data, as much of the data on the cloud may be encrypted

Secure object query processing of the data.

We are using normally Hadoop distributed file system for virtualization at the various storage levels and applying security interfaces for Hadoop which includes an XACML implementation and specifications. In addition ways, we are analyzing and investigating secure federated query processing on different clouds over Hadoop map reduces. These technical efforts will be described in the subsequent adjacent sections [9].

1.8 Security Issues for Clouds

There are numerous security issues for cloud computing as it encompasses many more technologies including such as networks and network alliance technologies, databases, operating systems, Virtual reality, virtualization, resource scheduling, transaction management system, load balancing, data traffic controls, concurrency control, conjunction control and memory management. Therefore, security issues for many of these related systems and technologies are applicable to cloud computing environment. For example, the connected network that interconnects the internal systems in a cloud has to be secure within existing environment.

Virtualization paradigm in cloud computing results in many security concerns. For example, mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. In addition, resource allocation and memory management algorithms have to be secure. Finally, data mining techniques may be applicable to malware detection in clouds [10].

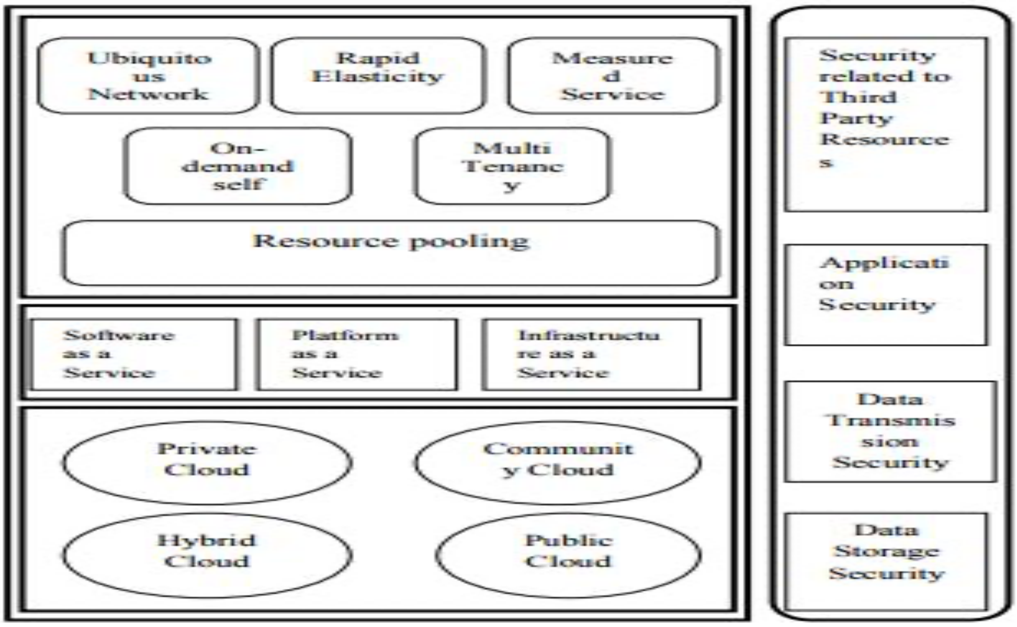


Figure 1:13 Complexity of security in cloud security environment

1.8.1 Techniques to secure data in cloud

Authentication and Identity: Authentication of customers or users and even of communicating systems is performed by different methods, but the most of cases used in cryptography technologies. Authentication of customers or clients takes place in different ways like in the form of passwords that is known individually, in the way of a security token, or in the form a various measurable identity quantities such as bio-metric, palm, passwords, eye-iris scan, voice or face recognition, fingerprint. One major problem with using traditional identity way approaches in a cloud computing environment is thoroughly faced, when an organization or enterprise widely uses multiple cloud service providers (CSPs). In such a way use case, synchronizing original identity information with the enterprise is not scalable. Other problems arise with traditional identity approaches when migrating infrastructure toward a cloud-based solution.

Data Encryption: If you are planning to store case-sensitive information on a huge data store then we need to use data encryption and decryption techniques. Having passwords and firewalls is good, but people can bypass or hack them to access your data in different ways. When your data is encrypted, it is in a way that cannot be read or access without an encryption security key. The data is totally useless to the intruder. It is a technique of translation of data into secret code. If you want to read the encrypted data, you should have the secret key or password that is also called encryption key [9].

Privacy and Information integrity: Cloud computing provides information and resources to valid customers or clients. Resources can be accessed through web browsers or various resources and can also be accessed by malicious attackers in different locations. A convenient solution to the problem of information integrity is to provide mutual trust cases between service provider and valid customer. Another solution can be providing proper channel ways such that security services, authentication, authorization and resources accounting controls, so the process of accessing required information should passes through different multi levels of validation stages to ensure the authorized use of existing resources. Some of the secured access mechanisms should be provided like RSA encrypted certificates, SSH based tunnels, Trusted third party gateways etc.

Availability of Information or Data: Non availability of information or data is a major problem or issue regarding cloud computing services; it does create dump space in cloud storage environment. Service Level agreement is used to provide the information or required data about whether the existing network resources are available for clients or not. It is a trust bond between customer and authenticated service provider. An ensure way to provide information availability of existing resources is to have a restore or backup plan for local resources as well as for most critical information. This enables the clients or customer to have the data about the resources even after their unavailability.

Secure Information Management: It is a famous technique of information security for a collection of data into central repository system. It is comprised of wages or agents running on systems that are to be monitored all operations and then sends necessary information to a cloud server that is called “Security Console operations”. The security console is managed and monitoring by administrator, who reviews the information and takes necessary actions in response to any related alerts.

As the cloud user base, dependency stack increase, queue operation module and the cloud security mechanisms to solve security issues also increase, this makes cloud security management much more complicated. It is also known as a Log Management. Cloud computing service providers also provide some of the security standards like a PCI DSS, SAS 70 and RCH 32. Information Security Management Maturity shares data another model of Information Security Management System through trusted third party authentication

Malware-injection attack solution: This solution creates a number of user’s virtual machines and stores all of data in a central storage. It utilizes FAT (File Allocation Table) consisting of virtual operating systems and cloud secure environment. The platform based application that is run by a valid user can be found in FAT table and NTFS. All the instances and objects are managed and scheduled by Hypervisor under virtual 7 controls. An Interrupt Descriptor Table (IDT) is used for integrity information checking and validation requires.

1.8.2 Cloud computing Security Standards

Security standards define procedure and processes for implementing a security program. In this way cloud environment maintain a secure public, private or hybrid environment, that provides Integrity, spam reduce, privacy and security Some reasonable steps are performed by applying cloud security related activities by these international accepted standards.

“Défense in Depth” is widely used in cloud computing to provide security. This concept elaborates different layers of defence. In this form, if one of the systems fails in this existing environment, secure overlapping technique can be used to provide security in various modules as it has no single point of failure at any cases. Traditionally, endpoints subscriptions have the technique to maintain security, where access is controlled by valid client.

1.8.3 Security Assertion Mark-up Language (SAML)

It is widely used in business and commercial deals for secure communication between online multiple partners. It is an XML or Java servlets based standard used for authentication, authorization among all the partners. SAML defines three roles:

The principal (a user)

A service provider (SP)

An identity provider (IDP)

SAML provides queries and various responses to specify client's attributes for validation, verification, and authorization and authentication information in XML format. The requesting trusted third party is an online demand site that receives various security information.

1.8.4 Open Authentication (O-Auth):

It is a general method used for associating and interacting with protected various data. It is initially used to provide data access to many kinds of developers. Clients or customers can permission grants and access to information too developers and customers without sharing of their personal identity. Open Authentication does not provide any security features by itself in fact it depends on other protocols like SSL to provide security.

1.8.5 Open Identity (Open ID) :

It is a single-sign-on (SSO) method. It is a secure common login process that allows clients or customer to login once and after use all the participating existing systems. It does not based on central authorization for authentication of clients or users. For example: Google, yahoo and in.com

1.8.6 SSL/TLS:

TLS is used to provide most secure communication over TCP/IP network. TLS works in generally three phases: In first phase, negotiation is done between valid users to identify which ciphers security keys are used. In second phase, Public key exchange algorithm is used for authentication and authorization process. These key exchange algorithms are public key algorithm and support existing resources under controlling. The final phase involves message encryption and cipher encryption. these encryptions are done through various retrieval process under circumstances.

1.9 SECURITY ISSUES

The security of corporate data in the cloud is difficult, as they provide different services like Network as a service (NaaS), Platform as a service (PaaS), Software as a service (SaaS), and Infrastructure as a service (IaaS). Each service has their own security issues.

1.9.1 Data Security:

It refers as a confidentiality, availability, reliability and integrity. These are the major possible issues for cloud service vendors. Confidentiality is defined as a privacy of information or data and designed to prevent the case sensitive information or data from unauthorized or unknown people. In this cloud stores the public encryption key data from various enterprises, stored at encrypted format in another enterprise, that data must be secure from the employees of enterprise database. Integrity defined as the exactly correctness of data, there is no common policies exist for approved data exchanges in existing cloud storage. Availability is defined as data is available on time during retrieval of data from cloud storage.

1.9.2 Regulatory Compliance:

Customers are eventually accountable when the security and completeness of their own data is taken by a service provider. Traditional service providers more prone to outsource surveys and security certification. Cloud computing providers reject to endure the scrutiny as signalling so these customers can only make usage of paltry operations.

1.9.3 Data Locations:

When users use, they probably won't know exactly where their data will hosted and which location it will stored in. In fact, they might not even know what country it will be stored in. Service providers need to be asked whether they will accomplish to storing and alter data in particular arbitration, and on the basis of their customers will they make a fair accomplishment to follow local privacy requirement [9].

1.9.4 Privileged user access:

Outside the resource data that is processed contains an indigenous risk, as deploy services, avoid the mortal, consistent and human resource manage IT shops works on the house programs.

1.9.5 Trust Issue:

Trust is also a major issue in cloud computing. Trust can be in between human to machine, machine to human, human to human, machine to human. Trust is revolving around assurance and confidence. In cloud computing, user stores their data on cloud storage because of trust on cloud. For example people use Gmail server, Yahoo server because they trust on provider.

1.9.6 Data Recovery:

It is defined as the process of restoring data that has been lost, corrupted or accident.

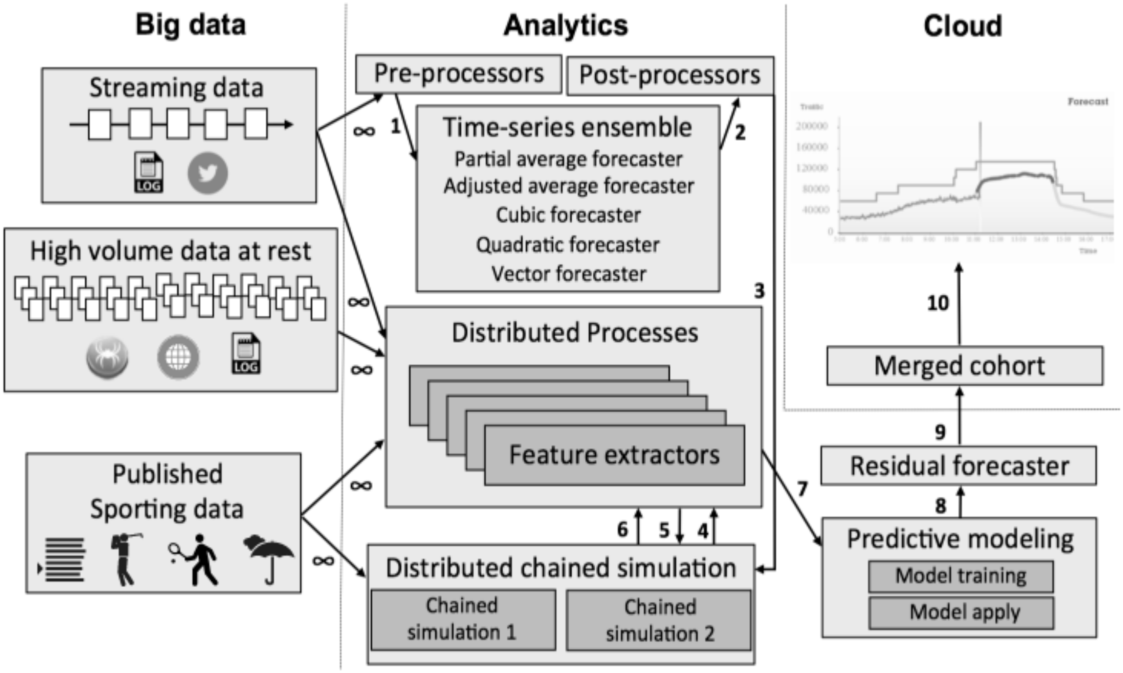


Figure 1:14 Data sharing process on cloud environment

1.9.7 Out sourcing:

Outsourcing brings down both capital expenditure and operational expenditure for cloud customers. However, outsourcing also means that customers physically lose control on their data and tasks. The loss of control problem has become one of the root causes of cloud insecurity. To address outsourcing security issues, first, the cloud provider shall be trustworthy by providing trust and secure computing and data storage; second, outsourced data and computation shall be verifiable to customers in terms of confidentiality, integrity, and other security services.

In addition, outsourcing will potentially incur privacy violations, due to the fact that sensitive data is out of the owner's control. Massive data and intense computation: Cloud computing is capable of handling mass data storage and intense computing tasks. Therefore, traditional security mechanisms may not suffice due to unbearable computation or communication overhead. For example, to verify the integrity of data that is remotely stored.

References:

1. Cloud security: risk factors and security issues in current trends Dr.K.Sai Manoj International Journal of Engineering & Technology, Science Publishing Corporation October 2019 (Scopus) https://www.sciencepubco.com/index.php/ijet/issue/view/495 (Indexed in German National Serials Database (ZDB) (Germany), ProQuest (USA) etc)

2. Conceptual oriented study on the cloud computing architecture for the full-security, Dr.K.Sai Manoj International Journal of Engineering & Technology, (SPC) https://www.sciencepubco.com/index.php/ijet/article/view/11654

3. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.376.3145&rep=rep1&type=pdf

4. Gerald Kaefer, Cloud Computing Architecture, Corporate Research and Technologies, MunichGermany,4th Generation Datacentre IEEE Spectrum,1-9,2010.

5. Dejun Wang, An Efficient Cloud Stoage Model for Hetrogeneous Cloud Infrastructure journal 1877-7058/10.1016,510-515,2011

6. Rajkumar Buyya1,2, Saurabh Kumar Garg1, and Rodrigo N. Calheiros,SLA-Oriented Resource Provisioning for Cloud Computing:Challenges,Architecture and Solutions,2011 International Conference on Cloud and Service Computing,1-10,2011.

7. Bhaskar Prasad Rimal · AdmelaJukan ·DimitriosKatsaros · Yves

Goeleven, Architectural Requirements for Cloud Computing, JOURNAL/10.1007/DOI 10.1007/s10723-010-9171-y,1-26,2011.

8. Campbell, Geronimo, “Applied Virtualization Technology,” Hillsboro, Intel Press (ISBN 09764832-3- 8), 2006, pp. 69-73.

9. Dong Xin, et al.”Achieving secure and efficient data collaboration in cloud computing. ”Quality of service, 2013 IEEE/ACM 21st International symposium on.IEEE, 2013.

10. Xia Z., Zhu Y., Sun X. and Chen L. (2014), "Secure semantic expansion based search over encrypted cloud data supporting similarity ranking "Journal of Cloud Computing”, Springer 3.1, pp. 1-11.

11. Risk Factors And Security Issues In Various Cloud Storage Operations Dr.K.Sai Manoj Volume-8 Issue-12, October 2019, ISSN: 2278-3075 (Online) Published By: Blue Eyes Intelligence Engineering & Sciences Publication (First Author) (Elsevier Scopus)

12. Dewan, H. and Hansdah, R. C., 2011. A Survey of Cloud Storage Facilities. 2011 IEEE World Congress on Services, 224–231.

13. Google, 2016a. Google Drive - Cloud Storage; File Backup for Photos, Docs & More [online]. Available from: https://www.google.com/drive/ [Accessed 5 May 2016].

14. Satran, J., Meth, K., Sapuntzakis, C., and Chadalapaka, M., 2004. Internet Small Computer Systems Interface (iSCSI). [online]. Available from: http://www.ietf.org/rfc/rfc3720.txt [Accessed 5 May 2016].

15. Miller, R., 2013. How Dropbox Stores Stuff for 200 Million Users. Data Center Knowledge, 2013–2016.

16. SpiderOak, 2016. SpiderOak [online]. Available from: www.spideroak.com [Accessed 5 May 2016].

17. Microsoft, 2016a. Microsoft OneDrive [online]. Available from: https://onedrive.live.com/about/en-us/ [Accessed 5 May 2016].

18. Microsoft, 2016b. Microsoft Azure: Cloud Computing Platform & Services [online]. Available from: https://azure.microsoft.com/en-us/ [Accessed 5 May 2016].

19. Amazon S3, 2016. Amazon Simple Storage Service (S3) — Cloud Storage — AWS [online]. Available from: https://aws.amazon.com/s3/ [Accessed 5 May 2016].

20. Google, 2016b. Cloud Storage - Online Data Storage | Google Cloud Platform [online]. Available from: https://cloud.google.com/storage/ [Accessed 5 May 2016

21. SpiderOak (SpiderOak 2016), Google Drive (Google 2016a), Microsoft Skydrive (Microsoft 2016a), or professional No-SQL databases such as AWS S3 (Amazon S3 2016),

22. Google Cloud Storage (Google 2016b) or Microsoft Azure (Microsoft 2)

Chapter 2

2 Chapter 2 : REVIEW ON THE STAEMENT OF THE PROBLEM

2.1 Problem Definition:

In today’s world, the wireless technology and Internet of things plays important role, the mobile devices like smart phones, mobile devices etc needs different wireless access. Hence the requirement of bandwidth and the computation of network also get increased rapidly. The mobile devices becoming smarter and intelligent and it further require many computation servers. The development of these applications is getting limited because of finite computation service. In addition this computation causes more delay and this delay is not suitable for the devices or application which is more delay sensitive. Considering the collaborative service cache strategy of storing such as storing demand among mobile users, the data size and the required computation capacity of task in service cache using MCC (e.g., the Increasing cache services in Mobile Cloud Computing and online intermediate storing processing have different storage and CPU requirements) and the Mobile Cloud Computing and storage constraints of Cloud in 5G cellular network, Maintain the energy in Cloud clouding is challenging problem. The main problem in caching is content caching and task caching therefore based on the caching method server should assign. Still Cloud with server setup not able to catch and store all type of computation storage. Normally Collaborative resource allocation method is defined in cache technique with three classification Voice User, data User, and Offloading user. Normal user adopts with spectrum utilization and data user generates utility due to spectrum and cache. Offloading user generates utility due to spectrum and computational resource. Every Base Station is connected with Mobile Cloud Computing Server for Computational task offloading and which is not consider the virtualization with interference in Neighbour Cloud to handle Interference issue.

In the processing of data offloading in multiple users and multiple servers, Mobile Cloud computing task can be processed on Cloud or locally in 5G Cellular network. Though, when the 5G cellular task is cached in the Cloud, it may not need to be processed locally in advance network. Based on the deciding task how much task to offloading is challenging issue. Thereafter, it is challenging to make a task offloading in data with task caching using advanced network.

Mobile Cloud Computing Optimization problem in 5G cellular network: When computing and storage resources at Cloud are limited, how to give task caching and offloading problem and solve this problem is challenging issue. This is because Mobile Energy Cloud computing multiple energy task caching and offloading scheme needs careful coordination

Open source in MCC, a user task has to be controlled to be offloaded to the right Mobile Cloud server with cache, in remote MCC, to get served. This offloading is facing a problem while finding the server and problem in service cache. There will be less implementation in service side and secure cache performance. In which server will be position to get the traffic and maintain the secure cache. Since we are facing problems in application security and delay time for responding. These are a need to develop the solution to fulfil all the problems mentioned in the research. Maintain the energy of the system will be tough one due to the task offloading.

Mobile Cloud Computing is developing recent years which provides this computation without delay and high performance by deploying Cloud servers in the mobile network. The Cloud servers compute the user requirement within fraction of second and it is very suitable for delay sensitive tasks. In order to decrease the delay and energy used for a computation the mobile Cloud computing requires two important aspects and they are

- Cloud Caching
- Task Offloading

Cloud caching application data is revealed and easy to access through unauthorized one. Cloud Cache data's has threat from hackers and leaking information

2.1.1 Problem of Secure Task Caching

Each task required by the various mobile devices will be different, and their computation requirements also are different, so the heterogeneity of the task and the computation need more cache space, which is a challenging face for the secure Cloud server.

2.1.2 Problem of Secure Task Offloading

When a computing task has assigned on the Cloud server, the Cloud server computes it locally. But if the task has cached in the Cloud, the task need not be performed locally. Hence the task offloading decision is a challenging task to make the system secure and energy-efficient.

Security Caching and offloading is a big challenging issue in Mobile Cloud Computing. Because of the limited storage, we need to carefully handle this problem of task offloading and task cache, which in turn decreases the energy consumed. The offloading cache task is challenging since the cache pollution attack has disseminated throughout the network, which will be a threat to secure communication.

2.2 Origin of the Problem

All through the 1990's the ascent of business enthusiasm for the Internet has led to the joining of the data foundation as a center part of the United States economy. Nonetheless, an expanding number of digital assaults and dangers of digital assaults on our national systems have indicated that our vitality, transportation, and fund frameworks are open to possibly desperate results. While a large division of these assaults has been insufficient, the Internet has become a field for fighting and demonstrations of fear-based oppression, since it controls different necessary frameworks. Securing these foundations has become an essential and key territory of enthusiasm for country barriers. Current digital security capacities have advanced to a great extent as patches and additional items to the Internet, which was structured on the standards of open correspondence and understood shared trust. This one currently perceived that it is never again adequate to pursue such developmental ways and that security must be a fundamental piece of the data foundation. Existing interruption location frameworks have advanced as discrete, specially appointed abilities and are not adequate for reacting to complex and masked digital assaults anticipated from well-supported psychological militant associations. It made a chance to build up another bearing on an enormous scale and coordinated interruption discovery and reaction frameworks, which is the fundamental inspiration for this paper [3]. Proposition the Machine learning, Data Mining strategies were depicted, and a couple of usages of each system to computerized interference identification issues. The diverse nature of different AI and data mining counts discussed. This research work points out the course of action of assessment criteria for AI and data mining methods. The game plan of recommendations on the best techniques to use depends on the qualities of the computerized Issue to handle Cybersecurity. It is the game plan of advances and methodology planned to guarantee PCs, frameworks, ventures, and data from ambush, unapproved access, change, or pounding. Computerized security frameworks made out of framework security frameworks and PC security frameworks. Each of these has, in any event, a firewall, antivirus programming, and an interference recognition framework. Intrusion discovery frameworks help find, choose, and perceive unapproved use, duplication, alteration, and pulverization of information frameworks.

The security breaks consolidate external interferences ambushes from outside the affiliation and inside interferences. There are three essential sorts of advanced assessment in the help of interference identification frameworks: misuse based, oddity based, and crossbreed. These are effective for perceiving known kinds of attacks without making a stunning number of bogus alerts. They require to visit manual updates of the database with rules and stamps. Misuse based methodology can't recognize novel attacks. Cloud-based techniques show the conventional framework and framework lead and understand peculiarities as deviations from ordinary direct. [4]

They are drawing in an aftereffect of their ability to perceive zero-day ambushes. The critical obstacle of irregularity-based techniques is the potential for high bogus alarm rates because previously covered framework practices requested as peculiarities.

This research fixates basically on advanced interference location as it applies to wired frameworks. With a wired framework, an adversary must experience a couple of layers of shield at firewalls and working frameworks or increment physical access to the frame. A remote framework engaged at any centre point, so it is regularly more helpless against vindictive ambushes than a wired framework. The Machine learning and data mining methodologies campaigned in this paper are material to the interference and misuse recognition issues in both wired and remote frames. The per user who needs a point of view focused just on remote framework protection suggested papers, for instance, Zhang et al., which focuses more on one of a kind changing framework topology, coordinating computations, decentralized organization, etc.

2.3 Related Work:

The essayists SongnianLi, Suzana Dragicevic, et al. conducted a study on various geospatial theories and procedures used to manage immense geospatial data. Given some unique properties, makers thought that standard data taking controlling ways of thinking and frameworks are missing. The going with spaces seen as in need of advancing progress and assessment in control. These wires the degrees of improvement in tallies to supervise the regular examination, develop flooding data, and improve new spatial requesting systems.

In Yuehu Liu, Bin Chen et al. have proposed another strategy for controlling monstrous remote identifying picture data by utilizing HBase and Map-Reduce framework. From the start, they have divided the certified picture into various little pieces, and store the squares in HBase, which dissipated in a social event of focuses [5].

They have used a Map-Reduce programming model to manage the set-away pieces, which simultaneously executed in a social event of focuses. The middle focuses on the Hadoop bunch have no necessities for predominant and precision with the objective that they can be unusually affordable. Likewise, in light of Hadoop's high flexibility, it is unquestionably not difficult to add new focuses to the gathering, which was regularly staggeringly problematic with everything taken into account ways. Finally, they see that the paces of data exchange and taking care of addition because the pack of HBase creates. The outcomes show that HBase is, to an incredible degree, reasonable for considerable picture information gathering and managing. The makers Chaowei Yang, Michael Goodchild et al. have foreseen a substitution paralleling limit and access strategy for huge scale NetCDF sensible information that is maintained liable to Hadoop.

The assessment result implies the parallel procedure utilized to store and recuperate the gigantic scale NetCDF gainfully. Huge data has changed into a noteworthy focal point of generally speaking interest that is coherently pulling in the assertion of the educated gathering, industry, government, and other association [6].

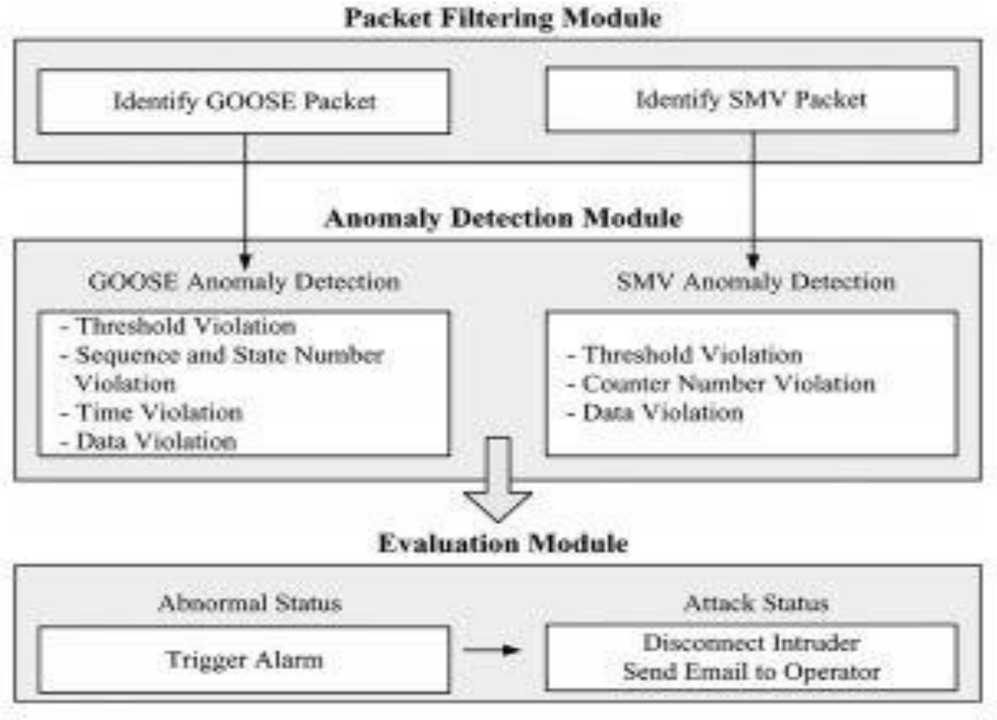


Figure 2:1 Packet filtering internal Process

This research pointed about inconsistency recognition at a substation. An incorporated technique for having based and arrange based oddity location plans proposed. The host-based irregularity location utilizes an efficient extraction procedure for interruption impressions that to recognize believable interruption occasions inside a substation, e.g., firewall, UI, IEDs, and circuit breakers. The system put together irregularity discovery is engaged for multicast messages in a substation arrange; it additionally identifies, in a continuous domain, oddities that exhibit anomalous practices. The fundamental commitment of this paper is another technique for

- An incorporated peculiarity discovery framework for the insurance of IEC 61850 based substation mechanization framework, e.g., IEDs, UI, and firewall, and
- A system-based irregularity location calculation utilized to recognize pernicious exercises of IEC 61850 based multicast conventions,

e.g., GOOSE and SMV, over the substation organize. Inconsistency location for multicast messages in substation mechanization arrange is another field of research for the power lattices. In this examination, Cybersecurity tested has been created and used to approve the proposed peculiarity identification calculations. Digital interruptions reproduced utilizing the tried, including defensive IEDs. The test outcomes exhibit that proposed abnormality recognition calculations are compelling for the identification ofrecreated assaults [5].

2.4 Technical Approach

We built up an incorporated cybersecurity system to recognize and contain digital assaults at the degree of hierarchical system space. This structure comprises of three parts: interruption discovery, assault source restriction, and assault regulation. For the first and third segments, we used the current techniques just as built up a few new parts. Specifically, we created novel data combination strategies for having level peculiarity discovery and for organizing level determination and assault source distinguishing proof.

Our coordinated system for interruption location and regulation accommodates versatility by enabling different sensor motors to work in parallel. Single system sensors can just deal with little traffic stacks and regularly constrained in their usefulness. Only by working in a conveyed manner can a large-scale approach be practical. This new approach works in a self-governing way that permits close to an ongoing reaction to occasions and to guarantee that the most recent mark refreshes are accessible to the sensors when they exist. Current interruption location frameworks are not self-sufficient and depend on human mediation as a critical piece of their activity, making them requests of size slower than required. An immediate human-on the up and up movement can't generally viably counter the more up to date digital assaults, exceptionally, at high system speeds. By utilizing a self-governing and dispersed structure that appeared in Figure 1, the sensor yields from different pieces of the authoritative system space can be quickly connected [6].

Our structure is fit for tending to the switches to set parcel channels and the firewalls to explicit square ports. Together they structure a functioning reaction that is actuated by the source detachment segment. For any presumed assault, its mark is acquired by the identification module, along with the natural ways prompting the districts of the assault source. This part enacts the channels and natural means from the assault source to deny entry rights to the assault bundles. Therefore, the degree of the assault's scope is contained. We researched two classes of assault control strategies. The first approach is appropriate for attacks that produce low degrees of traffic, such as unapproved logins. Here, the fusers can promptly trade information with sensors and actuate the firewalls nearest to the source to sift through the assault machine's bundles. This strategy, be that as it may, doesn't work on account of assaults that create high traffic, for example, a forswearing of administration assaults. To deal with these cases, in this system, the fuser grows the rate controls step by step from the close by channels to more remote ones [8].

Preparative assaults establish a developing subclass of digital interruptions that depend on relentlessly trading off hosts and utilizing them as platforms to assault different hosts. Specific sorts of worms (e.g., Code Red II) that sustain by spreading from host to have a place with this subclass. Facilitated disavowal of-administration assaults that gather zombies into a stockpile of traded off hosts to enact them at a later point, and spam generators that use a suite of bargained hosts to send email floods, have a place with this subclass. It is critical to detach the inception of assaults, which can recognize insider and outer attacks. In this paper, we present a dynamic system that uses the propagative design of these assaults to acquire useful issue source separation calculations by using the information (when accessible) of the sensor initiation times and assault proliferation times.

The primary attribute of this subclass of digital assaults essential to us is that the attack proliferates over the system by "tainting 'one host or hub after another. The other assault qualities could fluctuate altogether in the sort of host bargain. The procedure for picking and assaulting has, and the produced time and traffic scales could differ broadly. In some worm assaults, the objective is to engender quickly, regularly arbitrarily, to taint whatever number has as would be prudent [Weaver et al. 2003, Shankar et al. 2003].

This conduct brings typically about the old-style S-bend of the number of contaminated hosts: the pace of disease begins gradually during the underlying stage, rapidly turns out to be exceptionally high as the worm develops in quality, and afterward decreases when a large portion of the powerless targets undermined. Zombies that made for disavowal of-administration or spam assaults use an increasingly conscious methodology of trading off hosts without creating high traffic levels and ordinarily spread all the more gradually. Frequently insightful worms like Nimda and Code Red II check the nearby systems more now than they examine remote systems. The absence of information on the endeavor's inner system addresses proposes that such worms would choose a filtering technique and spread deliberately and not haphazardly inside the undertaking intranet [9].

Particular kinds of worms and preliminary periods of facilitated forswearing of-administration and spam assaults have a place. Side effects of such attacks are identified at the system sensors by bundle marks and traffic attributes, and at the hosts by execution corruptions and peculiar framework conduct. We indicated that data about worm spread occasions and dynamic sensor initiation times intertwined with the system primary data to:

a) Seclude the districts of the system that contain the first assault starting point, and

b) Anticipate the following arrangement of the target has. We built up the assault spread charts that caught over three kinds of data and tackled the source disconnection and

admonishing issues utilizing diagram calculations. As the assault spreads, its side effects are distinguished by the sensors situated at the hubs, which could themselves fluctuate in their abilities and execution. In light of the areas and enactment times of the sensors that recognize an assault, we indicated that the source could be confined, particularly inside the system's specific districts. We considered two sorts of sensors sent to acknowledge the side effects of cyber-attacks, in the particular host and system sensors.

Host sensors commonly recognize assaults by using bundle marks, framework trouble making and execution debasements, and strange traffic levels to and from the host. System sensors work on the traffic streams inside the region of switches, switches, and firewalls; they recognize assaults by examining bundle marks just as by watching oddity examples of individual and total traffic streams. These two sorts of sensors could give subjectively extraordinary data, which is commonly limited in either case.

A venture arranges sends a blend of host sensors and deliberately found system sensors. We created calculations to consolidate the data from different sensors and the essential network data to seclude the districts containing the assault starting point. Specifically, these strategies choose if the assault began outside or inside the venture; in the previous case, firewalls at entryway switches actuated to drop the assault parcels. In the last case, fitting neighborhood firewalls enacted to isolate the sources. We additionally created calculations to anticipate the following arrangement of potential objective hubs dependent on the present sensor data with the goal that nearby firewalls enacted early to counteract the further spread of assault [10]. The areas of traded off hosts, together with the condition of sensor enactments, give the auxiliary direction data about the attack to find. The sensor initiation times and the evaluated assault spread occasions give us the directional data about the assault proliferation. We combined the auxiliary and directional data to seclude districts of the system that contain the first assault source. Our techniques are viable for assaults that spread purposely and structure the class of topological worms that generally work in the intranet setting just as for attacks that target has haphazardly over the Internet; however, start inside the intranet. As is not out of the ordinary, the accuracy of seclusion and cautioning relies upon:

a) Areas of host and system sensors and

b) Arrange availability

Moreover, the degree of information about every one of these things can likewise have a critical effect both on the calculations and their exactness for separation and cautioning. We created engendering diagram models that catch the properties (i) and (ii). Utilizing the data about the features in (iii), we infer a reasonable subgraph used both for segregation and cautioning. Such a methodology, to be specified using a preparative diagram for finding, has been used in process plants [Ira et al. 1985], dynamical frameworks [Rao and Viswanadha 1987], and optical systems [Mas and Thiran 2000].

While these frameworks are unique to PC systems, they all offer specific basic properties that make it conceivable to take care of starting point detachment and admonishing issues. We expanded and adjusted the techniques created for chart-based frameworks [Rao 1993a, 1993b] to propagative digital assaults. These augmentations included recognizing and characterizing the significant properties of PC systems and digital assaults as an engendering chart, and afterward using the fitting diagram calculations.

An enormous number of interruptions, such as port sweeps, login endeavors, and support flood assaults recognized at the hosts by coordinating the headers and substance of system parcels with known marks. These systems are genuinely experienced and accessible as freeware, such as grunt, and framed a few segments of our design. While these techniques identify known assaults, another key issue in interruption recognition today is the capacity to recognize new assaults. The first approach to achieve this is the recognizable proof of oddities, in particular, distorted deviations from typical conduct, that covered up inside a foundation of ordinary action. Abnormality recognition is pivotal against new systems, for which no realized mark exists.

We built up a strategy for distinguishing the projects running on the hosts with bizarre framework calls; specifically, we use histograms of framework calls of a program as a mark. An identifier is prepared on-line on the host utilizing known projects and few assault programs [9].

Such a methodology recently utilized dependent on the Basic System Module (BSM) information that contains the framework calls made by a program. The strategies are dependent on k-closest neighbor and bolster vector machines utilized with great achievement. However, both these techniques left leftover forecast blunders.

We built up a data combination-based way to deal with preparing a few neural system locators, wherein these different indicators are intertwined with the closest neighbor rule to produce the last answer. These techniques are promising can be appeared to perform in any event comparable to the best among the finders intertwined. A crucial outcome in the locator hypothesis expresses that there is no single best indicator; however, each shows well under various conditions.

Our combination approach accomplishes the best execution among the accessible locators. By and by, be that as it may, the client must suitably-picked to perform such performance. We recently built up the closest neighbor projective fusers that appeared to beat the individual identifier. For the abnormality location part of our framework, we built up a client design on BSM information, which performed superior to the previous techniques on the DARPA benchmark test set [9]. This arrangement utilized a straight fuser to initially consolidate ten sigmoid neural systems and the closest neighbor rule. At that point, a meta-fuser dependent on the nearest neighbor projective combination strategy [Rao 2002] conveyed the join the first locators and the straight fuser. The resultant melded identifier scientifically appeared to perform at any rate just as the best blend of the indicators. This framework accomplished zero mistakes on the DARPA benchmark dataset, which is the best execution for this dataset [11].

2.5 Blockchain Cyber Security Vulnerabilities:

The Cybersecurity framework comprises of those components engaged with the assurance of arranged PCs and data from digital dangers. The goal is to stop, avoid, recognize, recoup from, and react to hazards on the Internet. The risks take an assortment of structures and incorporate unapproved access to or utilization of data assets. PC arrange assaults that deny, disturb, debase, or devastate data and system assets. The security foundation serves to ensure against these dangers and guarantee the privacy, credibility, trustworthiness, and accessibility of information [1]. Blockchain is an exchange database which contains data pretty much every one of the exchanges at any point executed before and takes a shot at the Bitcoin convention. It makes a computerized record of exchanges and enables every member on the system to alter the file in a verified manner, which shared over the appropriated network of the PCs.

For rolling out any improvements to the current square of information, every one of the hubs present in the system run calculations to assess, confirm, and coordinate the exchange data with Blockchain history. On the off chance that lion's shares of the hubs concur for the exchange, at that point, affirmed and another square gets added to the current chain. The Blockchain metadata is put away in Google's Level DB by Bitcoin Core customer. We can imagine Blockchain as a vertical stack having squares kept over one another and the bottommost square going about to establish the stack. The individual squares are connected and allude to the past square in the chain. The different squares are recognized by a hash, which created utilizing secure hash calculation (SHA-256) cryptographic hash calculation on the header of the square [2]. A square will have one parent; however, it can have different kid each alluding to a similar parent square subsequently contains same hash in the past square hash field.

Each square contains hash of parent obstruct in its own header and the arrangement of hashes connecting singular square with their parent square makes a major chain indicating the primary square called as Genesis square. Blockchain innovation (BT) is a decentralized exchange and information the executive's innovation that give security, secrecy, and information uprightness without including any third-party association responsible for the exchanges. BT has value the executives abilities by utilizing electronic receipt records for exchanges perform more than web Blockchain Technology is additionally individual functional in the fields of fund, Gaming, betting, store network, assembling, exchange, and e-commerce. BT framework is a changeless database of every single chronicled exchange put away as a computerized record. Moreover, all hubs (clients) on the circulated blockchain system can deal with the mutual record. Blocks are orchestrated inside chains, wherever the base square be the establishment of the stack, each square be connected to the former square within the chain. Using cryptographic hash calculations, each square is distinguished by a created hash. The square within the chain container include single close Relative Square, yet different youngster squares. A square contains a header, made up of an interesting hash of its parent obstructs that interfaces it with its parent squares, shaping a chain.

Block chain Technology framework be a computerized verification of proprietorship to fills in because a decentralized database framework, to which a ceaselessly developing rundown of exchange records is kept up, which contrasts starting conventional incorporated record frameworks [12].

The utilization of Blockchain Technology in Bitcoin, which was propelled during November 2008, is to a great extent liable for the developing enthusiasm for BT. Bitcoin, a decentralized peer-to-peer advanced cash, track every single computerized occasion in an open record. It records all exchanges with the purpose of be shared between taking part parties and is checked by an accord of members in the mutual framework. When the data has been recorded during an advanced occasion, it can't be modified. Along these lines, Bitcoin contains a constant and obvious record of each occasion. Regarding security, Bitcoin is profoundly questionable in the advanced money showcase. In any case, Block chain Technology has discovered a extensive scope of uses in both the monetary and non-financial areas. A Blockchain makes an appropriated agreement in the computerized world, furnishing substances with a safe stage that keeps up past records of advanced occasions by making a verifiable record in an open record.

Exercises related with Block chain Technology are ordered interested in (3) three classifications in the perspective of association along with availability:

(a) The First-Generation open (Blockchain 1.0),

(b) The Second-Generation open (Blockchain 2.0),

(c) The Third-Generation Private (Blockchain 3.0).

Blockchain 1.0 sends cryptographic forms of money in applications identified with money, for example, cash moves, money repayments, and advanced installments. Blockchain incorporates brilliant agreements for monetary market along with budgetary application, this classification handle additional way with straightforward money exchanges. It incorporates stocks, securities, advances, contracts, titles, shrewd properties, and keen agreements. The third classification applies to applications past monetary forms, money, and markets. It incorporates zones, for example, government, wellbeing, science, proficiency, culture, and workmanship. Hence, Blockchain inside this classification are viewed as private. Blockchain is a hopeful innovation that may well ease the danger of cyber-attacks coordinated toward a solitary end, which could cut downward whole system [14]. In any case, a coded interruption or framework weakness could enable increasingly negative outcomes to the security of the framework. For instance, if effective, an aggressor would obtain entrance not exclusively to the data put away at the purpose of assault yet additionally to all data recorded in the record. In this manner, security issues identified with Blockchain are basic as far as Cybersecurity, safety specialists require toward completely comprehend the degree as well as effect of the safety and protection moves identified with Blockchain previous to anticipating the possible harm starting an assault and confirm whether present innovation container survive diligent hacking endeavors [15].

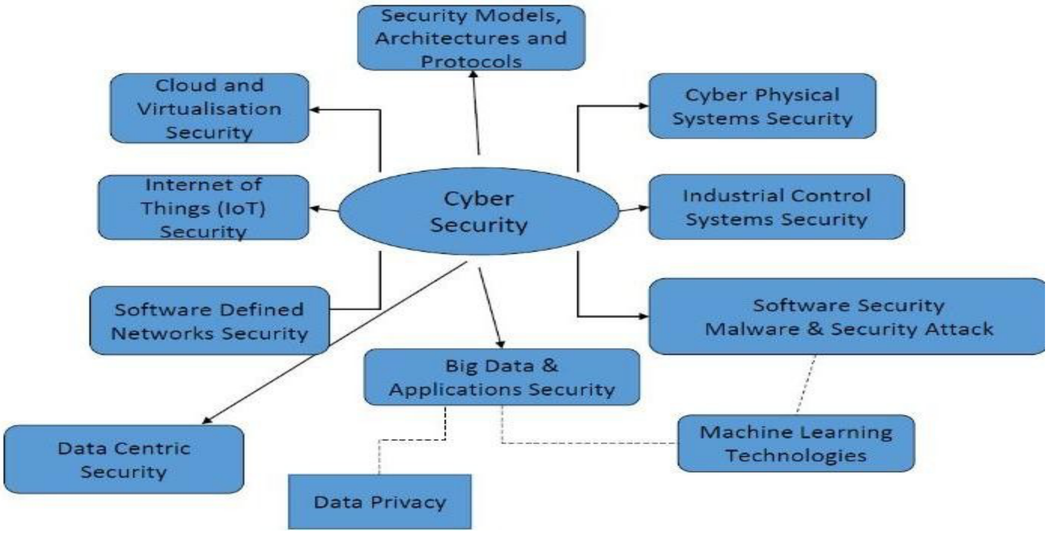

Security Models, Architectures and Protocols
Cloud and Virtualisation Security
Cyber Physical Systems Security
Internet of Things (IoT) Security
Cyber Security
Industrial Control Systems Security
Software Defined Networks Security
Software Security Malware & Security Attack
Big Data & Applications Security
Data Centric Security
Machine Learning Technologies
Data Privacy

Figure 2:2 Cyber Security approach related technological branches

Past examinations have investigated the specialized engineering of BT in connection to cryptographic money. Albeit a few examinations have concentrated on the security parts of BT, inferable from the expanding interest for cryptographic money by it’s present security challenges, these investigations have concentrated little on BT cybersecurity vulnerabilities. In view of such grounds, our examination shows an exhaustive survey of Block chain Technology security attacks by investigating assault vectors thatattention on client security and its attacks [14].

The above principles commitments of our examination are as per the following: first, initially investigation looks at safety measures difficulties and issues of existing digital currencies, together with the probability of assaults, concentrating essentially on issues of client protection and exchange obscurity. Their examination doesn't endeavor to fathom these difficulties and dangers, however rather exhibits a diagram of blockchain security, including looking at its vulnerabilities and talking about potential countermeasures.

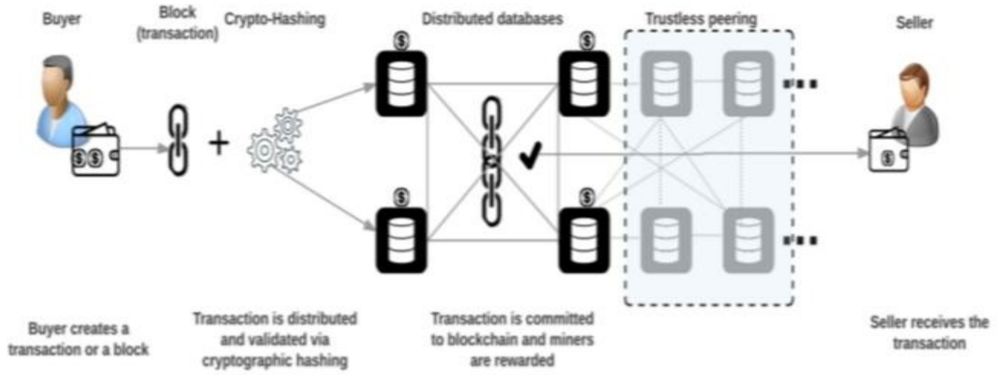

Buyer
Block (transaction)
Crypto-Hashing
Distributed databases
Trustless peering
Seller
Buyer creates a transaction or a block
Transaction is distributed and validated via cryptographic hashing
Transaction is committed to blockchain and miners are rewarded
Seller receives the transaction

Figure 2:3 Block diagram of Public Blockchain

2.5.1 Benefits of Bitcoin

- Fast and Cheaper: The exchanges made utilizing Bitcoin's wallets are quick and exchange expenses are insignificant.
- Decentralized Registry: Bitcoin cash is decentralized and no focal authority has full control and thus focal government or banks can't remove it from you and there is no chargeback. In any case, this is unimaginable with Bitcoins since the money is decentralized.
- Secure Payment Information: A Bitcoin exchange utilizes an open key and a private key. At the point when a Bitcoin is sent, the exchange is marked by open and private keys together which makes a declaration.

2.5.2 Network-level attack

At here, Blockchain arrange safety issues to turn into the majority well-known research issue in the system safety measures ground. In any case, present be as yet different worries about its adaptability, security, accessibility, and manageability. With the ascent of the advanced money advertising, digital assaults that try to impact promoting and business-oriented administrations are always expanding. Among the various assaults, conveyed forswearing of administration (DDoS) assaults is one of the most widely recognized system data transfer capacity utilization assaults that have messed up administrations. DDoS assaults on blockchain-based stages dislike normal assaults, and in a decentralized and peer-to-peer innovation, it is supplementary troublesome and exorbitant than in customarily dispersed application design when an undertaking toward stifle the system utilizing an enormous volume of little exchanges happens. Be that as it may, blockchain-based stages.

In this manner, flexible along with decentralized blockchain arrangements can offer high availability, yet DDOS assaults resolve stay a decided threat to security. In a digital money environment, cash trades assume a foremost job, yet by and large, these frameworks experience DDoS assaults all the more as often as possible. Feder et al expressed that few cash trades have been closed down because of DDOS assaults. Mt. Goex is one of the principal trades to handle over 75% of bitcoin exchanges around the world [13].

It is the main Bitcoin mediator and is measured the greatest Bitcoin trade. EVasek along with Mooere did a extensive observational investigation of DDOS assaults in the Bitcoin biological system along with announced 58 assaults on trades and Bitcoin administrations. Specifically, present contain be 250+ one of a kind DDoS assaults on 40 Bitcoin administrations, where 7% of every single realized administrator has confronted assaults.

The creators additionally information to trades, mining pools, betting administrators, wallets, and budgetary administrations are undeniably more powerless against DDoS assaults than different administrations are. Different reports show that 19.1% of little mining pools have been influenced by DDoS assaults, while 56.8% of enormous pools have confronted comparative assaults.

Thier contrasted a legitimate methodology and an exploitative technique. Under the legitimate Paradigm, players of an alliance could put resources into extra figuring assets to improve the probability of winning the following race. Untrustworthy performer alliances concentrated on a mining group and set off an exorbitant DDoS assault to bring down the normal accomplishment of a contending mining pool [17].

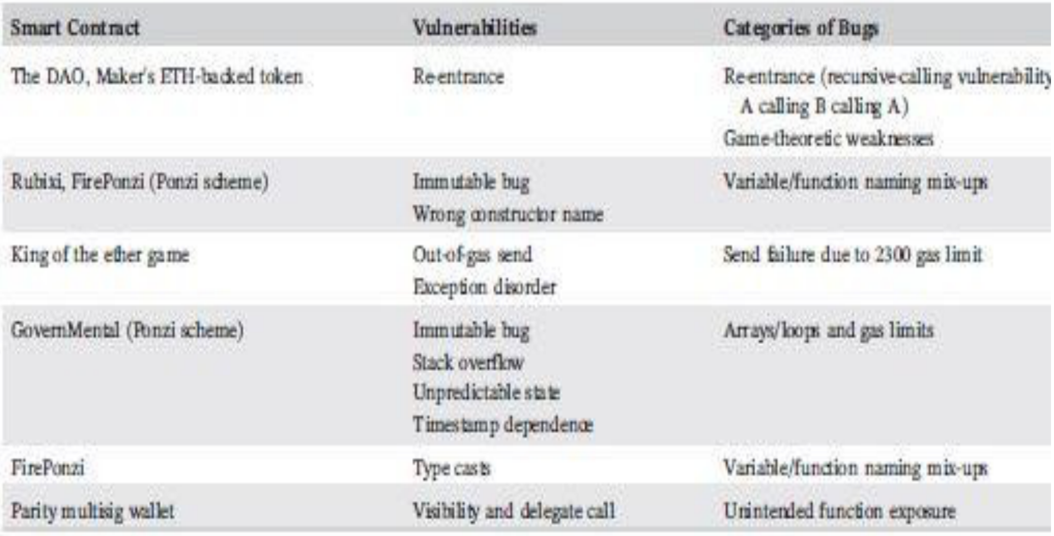
2.5.3 Block Producers Plan

Hypothetically, inside several Blockchain frameworks, and danger of BP's (diggers, validate) conspiracy is approaching. In light of DPoS transferred a few validations, it is constantly conceivable to compose intrigue between them. As per vitalik, more than two significant assaults could dispatch within individuals conspiring BPs:

restriction, change framework parameter, and twofold spend assaults.

2.5.4 Censorship Attack:

Although a framework is at last intended in the direction of energize competitions and agreement between BPs, there is no assurance for engineers along with clients that their applications and exchanges won't be there edited. Oversight assault beside to DPoS implies that BPs will not procedure legitimate exchanges. On the off chance that solitary a solitary BPs (or minor gathering) edits an entity, it won't be a major issue for the system.



Smart Contract	Vulnerabilities	Categories of Bugs
The DAO, Maker's ETH-backed token	Re-entrance	Re-entrance (recursive-calling vulnerability A calling B calling A) Game-theoretic weaknesses
Rubixi, FirePonzi (Ponzi scheme)	Immutable bug Wrong constructor name	Variable/function naming mix-ups
King of the ether game	Out-of-gas send Exception disorder	Send failure due to 2300 gas limit
GovernMental (Ponzi scheme)	Immutable bug Stack overflow Unpredictable state Timestamp dependence	Arrays/loops and gas limits
FirePonzi	Type casts	Variable/function naming mix-ups
Parity multisig wallet	Visibility and delegate call	Unintended function exposure

Table 2-1 Categorization of Various Attacks

2.6 Changing system parameters:

In DPOS, all progressions have to be activated through dynamic partner authorization, in fact, conceivable to BPs intrigue along with modify their convention parameter singularly. On the off chance that an assault is a triumph, at that point, the assailant (or aggressor gathering) possibly will change the formation, expanding their square rewards, fork out specific partners, along with different choices on the convention. The edge for changing the standards is equivalent to supplanting 51% of the chosen observers. The more partner support in choosing observers, the harder it become to modify the standards. DPoS is planned so that these assaults are unrealistic without understood voter endorsement. In the EOS cases, changes near convention parameter contain time delays before they are really consolidated. Likewise, endorsement by 17/21 BPs is required to change the constitution, and they should keep up that endorsement for 30 back to back days before the progressions could happen. In the event that the client doesn't acknowledge transforms, they can remove that BPs during that time and supplant them with makers that don't bolster the changes. At last, change the guidelines relies on everybody happening the system to overhaul their product, and no blockchain level convention can authorize, how system are altered. This implies hard forking "bug fixes" can be turned away lacking require a vote of the partners, in as much as they stay consistent with generally anticipated conduct of the code. By and by, just security-basic hard-forks ought to be actualized in such away. The designers and witnesses should trust that the partners will endorse even the most minor changes [17].

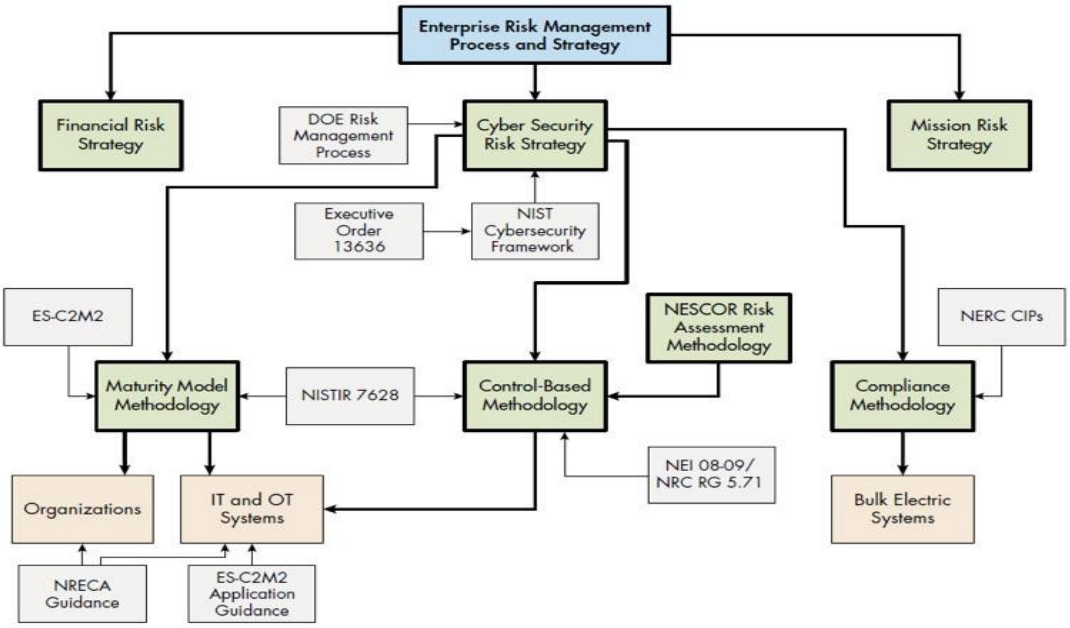

Enterprise Risk Management Process and Strategy
Financial Risk Strategy
DOE Risk Management Process
Cyber Security Risk Strategy
Mission Risk Strategy
Executive Order 13636
NIST Cybersecurity Framework
ES-C2M2
NESCOR Risk Assessment Methodology
NERC CIPs
Maturity Model Methodology
NISTIR 7628
Control-Based Methodology
Compliance Methodology
NEI 08-09/ NRC RG 5.71
Organizations
IT and OT Systems
Bulk Electric Systems
NRECA Guidance
ES-C2M2 Application Guidance

Figure 2:4 Cyber security monitoring process

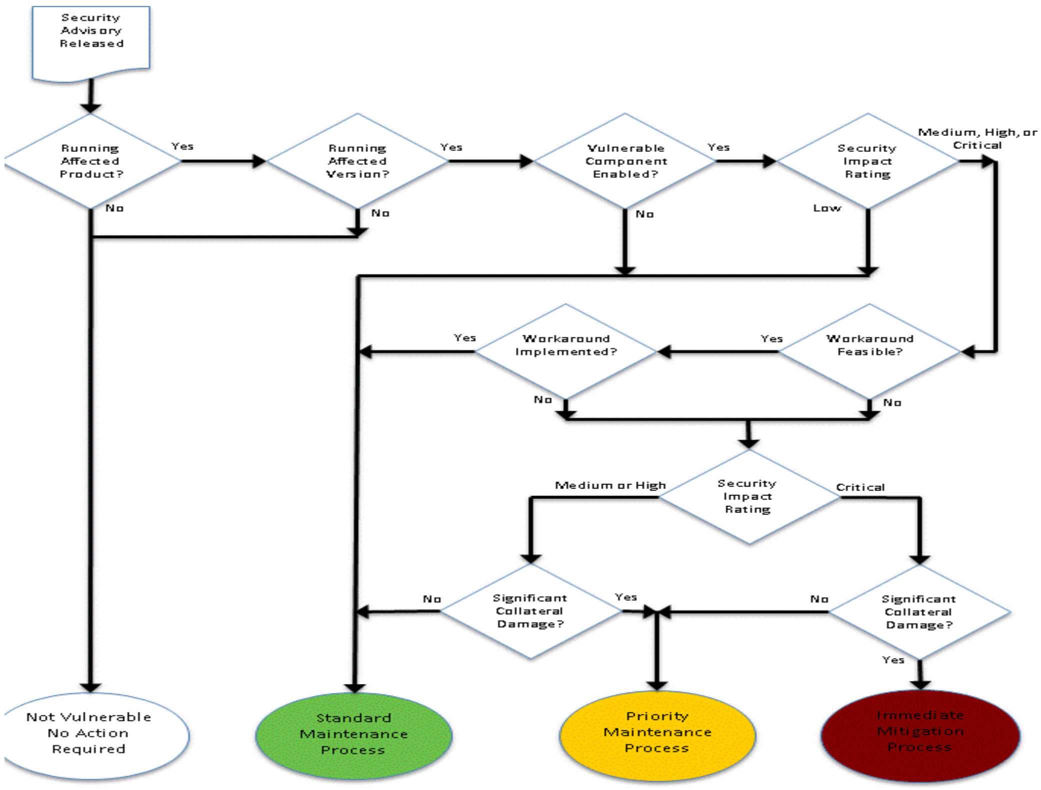

Security Advisory Released
Running Affected Product?
Yes
No
Running Affected Version?
Yes
No
Vulnerable Component Enabled?
Yes
No
Security Impact Rating
Medium, High, or Critical
Low
Workaround Implemented?
Yes
No
Workaround Feasible?
Yes
No
Security Impact Rating
Medium or High
Critical
Significant Collateral Damage?
No
Yes
Significant Collateral Damage?
No
Yes
Not Vulnerable No Action Required
Standard Maintenance Process
Priority Maintenance Process
Immediate Mitigation Process

Figure 2:5 Block Diagram of Risk Analysis

It has not yet been seen by and by; be that as it may, on the off chance that it occurs, the suggestions merit considering. On the off chance that BP's is required toward exist inside committed server farms, they restrict the quantity of possible BP's and particularly restrains the number of elements to can step within near supplant BPs to sbe removed. In the event that there isn't any BPs with adequate assets to supplant BPs that has been removed, at that point, thus, the system may endure. Voters would need to settle on rebuffing a making trouble BPs and bringing down the general assets of the system [17].

Governmental:

GovernMental encounter experiences a comparable issue, through subway methods, the agreement be ponnzi conspire. Clients would send the agreement through guarantee of an expanded return and with the opportunity to win a "big stake."

The agreement put away it's clients' locations inside a powerfully measured cluster along with expected toward repeat more than the exhibits so as near patent them at what time a big stake be strike. In any case, it didn't constrain the size of the cluster. Legislative in the long run pulled in enough clients that the gas allotment couldn't cover the whole exhibit [14]. Therefore, it would always neglect to reset the game and grant the big stake to the victor, with agreement's state remained successfully solidified.

Wallet security (private key security):

By and large, cryptographic forms of money store their incentive in a document store called a wallet, whereby every customer claims a lot of private-open keys to get to the wallet. The significant shortcoming with the wallet is that it very well may be impacted, squeezed, and migrated simply like different stores. Clients regularly neglect to review their defensive PIN or secret phrase or lose the hard drive where the private key is found. This implies a client may not generally have the option to get to their store [18]. Considering this, ransoms are can cause a similar issue.

Wallet burglary utilizes exemplary instruments, for example, phishing, which incorporates framework hacking, the establishment of surrey programming, and the erroneous utilization of wallets. A blockchain framework can without much of a stretch be abused through any powerlessness that may add to a cryptographic arrangement since clearly any program bug otherwise absence of protected private key be able to establishment of a significant safety break. Speculatively, a crypto assailant ought not toward have the option to comprehend the first plain content, which is encoded. Be that as it may, it isn't hard to comprehend the arrangement of the squares, and even a decent cryptograph makes a plain book, for example, irregular babble, however positive characters or numbers are frequently establish in a similar spot within every square in the Blockchain. This permits assailant the chance near endeavor a halfway portrayal of the natural content into each crypto secured square, where each square is an element of the former square [6]. In the cryptographic money space, Bitcoin has the biggest piece of the overall industry, wherever a Bitcoin file utilizes an open key, private key, and an individual location. As indicated by VanDam and Shparlinski, open keys can be produced securely from private keys utilizing a calculation called elliptic bend computerized signature (ECDSA). In any case, Vedral and Morikoshi contend that quantum PCs can break ECDSA. Furthermore, a machine can misuse quantum irregularity since its hidden truth is as yet obscure. This could permit the nearness of quantum bits (qubit), just as calculations that quantum PCs can play out that traditional PC can't. For instance, a quantum PC can run Shor's calculation and rapidly break any open key encryption by finding the elements of enormous numbers.

Unexpectedly, the Bitcoin convention address is determined to utilize the SHA-256 work for open keys, utilizing the RIPEMD-160 hash work and including a checksum for mistake remedy. While the scientific shortcomings of SHA-256 are astounding, no SHA-256 splitting episodes have happened, and subsequently, it has a solid and unsurprising future.

References:

1. Data Mining and Machine Learning Techniques for Cyber Security Intrusion Detection International Journal of Engineering and Advanced Technology (IJEAT) Dr.K.Sai Manoj Dr.P.S.Aithal ISSN: 2249 – 8958, Volume-9 Issue-3, February, 2020 https://www.ijeat.org/download/volume-9-issue-3/
2. Blockchain Cyber Security Vulnerabilities and Potential Counter measures International Journal of Innovative Technology and Exploring Engineering (IJITEE) Dr.K.Sai Manoj Dr.P.S.Aithal ISSN: 2278-3075, Volume-9 Issue-5, March 2020 http://www.ijitee.org/wp-content/uploads/papers/v9i5/E2170039520.pdf
3. Factom Partners With Honduras Government on Blockchain Tech Trial,http://www.coindesk.com/factom-land-registry-deal-hondurangov ernment/
4. Blockchain Adoption Moving Rapidly in Banking and Financial Markets: Some 65 Percent of Surveyed Banks Expect to be in Production in Three Years, https://www- 03.ibm.com/press/us/en/pressrelease/50617.wss
5. Bitcoin Developer Guide,https://bitcoin.org/en/developer-guide#blockchain-overview
6. The Blockchain,http://chimera.labs.oreilly.com/books/1234000001802/ch07.html/
7. Cyber Crime Costs Projected To Reach $2 Trillion by 2019, http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crimecost s-projected-to-reach-2-trillion-by-2019/#768e4f293bb0

8. Tendermint: Consensus without Mining, http://tendermint.com/docs/tendermint.pdf

9. What is Ethereum, https://cryptocrawl.in/what-is-ethereum/

10. Will Knight, “Anti-Snooping Operating System Close to Launch,” NewScientist, (May 28, 2002).
11. Riptech Internet Security Threat Report(January 2002). www.riptech.com.
12. Stock B., Göbel J., Engelberth M., Freiling F. C., and Holz T. Walowdac-analysis of a peer-to-peer botnet. In Computer Network Defense (EC2ND), 2009 European conference on IEEE; 2009:13–20.
13. Vedral V, Morikoshi F. Schrödinger's cat meets Einstein's twins: a superposition of different clock times. Int J Theor Phys. 2008;47(8):2126-2129.
14. Zheng Z, Xie S, Dai H, Chen X, Wang H. An overview of blockchain technology: architecture, consensus, and future trends. In: Big data (BigData congress), 2017 IEEE international congress on. IEEE; 2017:557-564.
15. S.King S, Nadal S. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. self-published paper; 2012.
16. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system, https://bitcoin.org/bitcoin.pdf, retrieved on 28/04/2018 Yli-Huumo J, Ko D, Choi S, Park S, Smolander K. Where is current research on Blockchain technology?—a systematic review. PLoS ONE. 2016;11(10):e0163477. https://doi.org/10.1371/journal.pone.0163477
17. Petar T., Andrei D., Drachsler C., Arthur G., Florian B. Securify: Practical Security Analysis of Smart Contracts. arXiv:1806.01143v1 [cs.CR]. 2018
18. The Finney Attack, Available from https://bitcoincoreacademy.com/the-finney-attack, retrieved on 28/04/2018

Chapter 3

3 Chapter 3 : Review of the Literature

Review of the Literature

Literature Review, explains detailed process followed in selecting, sorting and describing extracted information. Scholars have proposed numerous Cybersecurity systems. In recent years, research analysis with results has been provided in the form of a literature survey and concluded the existing cybersecurity mobile cloud computing experiments. This research work investigation begins with the observation of cloud computing techniques, security-related things, an extensive literature on the innovative methods related to the cybersecurity system.

Categories of Security Challenges in Cloud Computing based pointing to my research work

Cloud computing security is the major concern and has various challenges that need attention [1][2]. From the recent surveys on IT executives and CIOs conducted by IDC, it was clear that security was the highly cited (74%) challenge. in the cloud computing field [3][4]. A comparison with grid computing systems also proves that for cloud computing security the measures are simpler and less secure [5]. Security in cloud computing is totally based on the cloud service provider, who is responsible for storing data and providing security [6].

Data Security

Information from articles that discuss about data security and data protection are considered.

Security provided by cloud SP’s might not be highly cost effective when implemented in small companies. But when two or more organizations share a common resource there is a risk of data misuse. In such situation it is required to secure data repositories [23]. Not only the data repositories but also data should be secured in any stage such as storage, transit or process [9]. Since this kind of sharing resources is prevalent in the CC scenario, protection of data is important and is the most important challenge among other CC challenges [17][18][19]. In shared areas to keep data secure is challenging than protecting in a personal computer [20][21]. This problem has begun due to the introduction of new paradigm CC [10]. The author of article [31] explains how data security effects in various service models namely SaaS, PaaS and IaaS and in the article [6] author advocates that data security is the primary challenge for cloud acceptance and author for [10] expresses that cloud data security is an issue to be taken care of. For enhanced security on data repositories, it is important to provide better authentication, authorization and access control for data stored on CC in addition to on-demand computing capability [38][28][13].

Given below is the key area in Data security that CC refers to [16]:

Confidentiality: When enterprise data is stored outside organizational boundaries it needs to be protected from vulnerabilities. To protect data from vulnerabilities, employees must adopt security checks to ensure that their data stays protected from malicious attacks [10][2][40]. Few tests are used to help organizations to assess and validate, to which extent data is protected from malicious user and they are as follows [41][26][18][15]:

(a) Cross-site scripting [XSS]

(b) Access control weaknesses

(c) OS and SQL injection flaws

(d) Cross-site request forgery [CSRF]

(e) Cookie manipulation

(f) Hidden field manipulation

(g) Insecure storage

(h) Insecure configuration

In 2011, Mr.Jan de Muijnck-Hughes concluded a cyber-security analysis technique identified as Predicate Based Encryption (PBE). The security system contains PBE, and it speaks to a group of data encryption and starts from Identity-Based Encryption [1]. This technique coordinates Attribute-Based Access Control (ABAC) with lopsided encryption, in this manner, permitting a prime encryption/multi decryption environmental factors to be understood the use of a top plan. This Predicate Based Encryption focuses its execution at every platform as assistance and software as a help. This proposed approach additionally blocks undesirable presentation, unfortunate spillage and other unwanted ruptures of secrecy of cloud inhabitant information

In 2011 Venkata Sravan et.al. Wrote a paper titled Cyber Security Techniques for shielding information in Mobile Cloud Computing. This paper aims to grasp the safety threats and establish suitable cybersecurity techniques that won't mitigate them in Mobile Cloud computing [2]. The analysis is known as a complete range of security challenges and cybersecurity techniques. The foremost measured attribute is confidentiality, followed by Integrity and convenience [2].

In 2011 Ali AsgharyKarahroudy wrote a paper titled Security Analysis and Framework of Cloud Computing with Parity Based Partially Distributed File System. This paper proposed a technique called Partially Distributed File System with Parity (PDFSP), which is a protocol developed as a modification on the existing GFS/HDFS [3]. This PDFSP has four main components; Client Access Machine, User Public Machine, Cloud Management Server, and File Retrieval Server. All these components work together to ensure data being transmitted does not get into the wrong hands. This paper addressed the three aspects of security, which are Confidentiality, Integrity, and Availability.

In 2013 Mr.Nabil Giweli proposed a concept based approach that describes the Cloud Computing Data-Centric Security approach. This proposal concentrates on providing data security at the data transmission level; hence the data are self-describing, self-defending, and self-protecting during their lifecycle in the cloud environments. This approach gives the entire responsibility to the data owner to set and manage cyber secrecy and data responsibility. This proposed solution based on the Concept Recall System (CRS), and it utilizes data symmetric and asymmetric encryption techniques. In this paper, the proposed solution proved to be very efficient as it does not require complex essential derivation methods, and the data file does not need to be encrypted more than once [4].

In 2013 Miao Zhou outlined five techniques to provide security and integrity of data in cloud computing. These techniques include; Innovative tree-based key management scheme, privacy-enhanced data outsourcing in the cloud, privacy preserved access control for cloud computing, privacy-enhanced keyword to search in clouds, and Public remote integrity check for private data. This paper adopted Keyword Searching Mechanism, which enables efficient multi-user keyword searches and hides the private information in the search queries [5]. An encryption scheme for a two-tier system presented to achieve flexible and fine-grained access control in the cloud. The experimental results indicated that the proposed project is efficient, especially when the size of the data file is large, or the integrity check is frequent [5].

In 2014 Sudhansu Ranjan Lenka et al. proposed a paper titled "Enhancing Data Security in Cloud Computing using RSA Encryption and MD5 Algorithm. As the title of the article suggests, they implemented both RSA Algorithm and the MD5 algorithm. In this paper, the RSA Algorithm used for secured communication and file encryption and decryption purpose. In contrast, the MD5 algorithm is used for digital signature and covers the tables for unauthorized users [6]. The two algorithms proposed provides the three key aspects of security, which are Confidentiality, Integrity, and Availability.

In 2014 Aastha Mishra proposed concept intelligence of secure sharing key process scheme. This paper aims to introduce a more reliable decentralized lightweight essential management technique for cloud systems that provide more efficient data security and key management in cloud systems [7]. Security and privacy of user's data are preserved in the proposed technique by the replication of significant share among several clouds by the use of a secret sharing approach and using a voting method to check the Integrity of shares. In this paper, the technique used also brings to bear better security against Byzantine failure, server colluding, and data modification attacks [7].

In 2014 Nesrine Kaaniche proposed a paper titled; Cloud Data Storage Security based on Cryptographic Mechanisms. In this paper, Nesrine proposed two techniques to secure data which are ID-Based Cryptography (IBC) and cloud security. With ID-Based Cryptography, the paper proposed to use each client as a private key generator which generates his own ID-Based Cryptographic Public Elements (IBC-PE). These IBC-PE are used to compute ID-based keys and also serve to encrypt the data before their storage and sharing in the cloud [8]. Concerning CloudaSecurity, there is a public key-based solution that proposes the separation of subscription-based key management and confidentiality oriented asymmetric encryption policies [8]. In this portion, the author intended two techniques to maintain security for mobile cloud data: ID-Based cyber data Cryptography and Cloud security. With the concept of cloud-based ID-Based Cryptography, the proposed method is used to secure the client based private key generator, which provides their security standards. These cybersecurity standards will maintain the ID-based keys and serve the encrypt data and store it in the cloud and share it with the clients. The cloud-based subscription key will generate the equal duration of the subscription, and the key will be made by the customer who would accept it. Every sequence of time interval the data will be shared to the client based on the private, secure key and key will address will be in the binary level. The client details maintained in cloud computing and data subscription will be processed through mobility as well. The mobile data communication will be under secure packet transmission. The subscription scheme provides data storage provision, which we will encourage data to upload computational concepts. The network will stream the data and provide fast access to clients based on internet speed.

In 2014 Afnan Ullah Khan wrote a proposal that Confidential data access method. In this research paper, the patient health status updated in the cloud and data owner or authorized controller will access the data through a security key based novel scheme. The idea of this concept would secure the patient data in the different scenarios in the Medical / Health care field where out of the data controller will not accept the data. The cybersecurity system provides security for various aspects of the data stored in multiple places and access through cloud computing. Data Consumers (patients, nurses, doctors, etc.), Infrastructure Providers, and Trusted authority would maintain private keys, which will provide security for the system. In contrast, cyber data confidentiality and data access authentication was achieved through the novel technique.

In 2016 Sarojiniet.al proposed a technique known as Enhanced Mutual Trusted Access Control Algorithm (EMTACA). This technique presents a mutual trust for cloud users and cloud service providers to avoid security-related issues in cloud computing [10]. This paper aims to propose a system that includes the EMTACA algorithm, which can assure enhanced guaranteed and trusted and reputation-based cloud services among the users in a cloud environment [10]. The results of this paper showed data confidentiality, integrity, and availability, which are the three most important aspects of data security was achieved.

In 2017, Dimitra A. Georgiou proposed security policies for cloud computing. The purpose of the security policies is to protect people and information, set rules for expected behavior by users, minimize risks, and track compliance with regulation [11]. The paper focused on software as a Service. The paper presented a detailed review and analysis of existing studies as far as security is concerned in cloud computing. With Dimitra's review of existing threats, he focused on the once that do not apply to conventional systems [11]. To be able to identify new rules that supposed to be integrated into the cloud policy, a methodology was proposed for assessing different threats in the cloud. This paper scrutinized the security requirements of a cloud service provider, taking into consideration a case study of Europe's E-health system.

In 2018 Dr.K.Sai Manoj investigated on the cloud computing architectures for the full-security [12]. Many developers have designed their architecture for installing the cloud computing infrastructure. The existing cloud computing architectures differ in many ways. Security has been a severe Issue as client-related data and processing is undertaken using the infrastructure provided by third-party service providers varies greatly. It is necessary to know the extent of the inclusion of security into the cloud computing system and then find the best architecture that includes the best and secure security system. In this paper [12], a comparison of existing architectures from the perspective of inclusion of security infrastructure within cloud computing system is presented along with a comprehensive architecture that is included with every aspect of security taking into account the most of the vulnerabilities

In 2019 Dr.K.Sai Manoj proposed [12] a conceptual oriented research paper on cloud computing. It is an emerging and way of computing in computer science. Cloud computing is a set of resources and services that are offered by the network or the internet. Cloud computing extends various computing techniques like grid computing, distributed computing. Today cloud computing is used in both industrial, research, and academic field. Cloud facilitates its users by providing virtual resources via the internet. As the field of cloud computing is spreading the new techniques are developing. This increase in the cloud computing environment also increases security challenges for cloud developers. Users of cloud save their data in the cloud; hence the lack of security in the cloud can lose the user's trust. In this paper, we will discuss some of the cloud security issues in various aspects, such as multi-tenancy, elasticity, reliability, availability, etc. In various sectors, the paper also discusses existing security techniques and approaches for a secure cloud environment. This paper will enable researchers and professionals to know about different security threats and models and tools proposed

In 2019 Dr.K.Sai Manoj had done active research [14] on Risk Factors and Security Issues in Various Cloud Storage Operations. Cloud computing is a rising and method for registering in software engineering. Cloud computing is an arrangement of assets and administrations that are offered by the system or web. Distributed computing broadens different figuring methods like framework registering, appropriated processing. Today distributed computing is utilized as a part of both mechanical, research, and academic fields. Cloud encourages its clients by giving virtual assets through the web. As the field of distributed computing is spreading the new procedures are producing for cloud security. This expansion in distributed computing conditions likewise expands security challenges for cloud designers. Customers or Users of cloud spare their information in the cloud subsequently the absence of security can lose the client's trust. In this paper, we will discuss cloud database and information mining security issues in different viewpoints like multi-occupancy, flexibility, unwavering quality, accessibility on different divisions like modern and research regions, and examine existing security methods and methodologies for a safe cloud condition through enormous information ideas. What's more, this paper additionally studies different parts of mechanical, training, and research areas. This paper will empower scientists and experts to think about various security dangers, models, and apparatuses proposed in existing distributed storage.

In 2019 Dr.K.Sai Manoj Proposed [15] Conceptual based Data Mining Techniques for the Prediction of Hydration Assessment, Breath Analysis, and Heart Disease —Both the facts mining and medicinal offerings corporation have risen some of robust early area frameworks and amazing well-being associated frameworks from the scientific and locating facts. With the fast development of health-associated facts advances, it's miles quite simple for the health care providers to examine and save extremely good measures of Patent data. For the effective usage of these statistics for the improvement of the best outcomes within the medicinal services and manner, properly-being professionals need to differentiate the best measures and comply with the proper research techniques for the sort of statistics within acquire. This audit Paper has merged at the information-digging strategies for the evaluation of Hydration reputation via Breathe examination and usage of data digging structures for the expectancy of heart sickness.

Dr.K.Sai Manoj was done active research on the Security Policies for Cloud Computing [16] -The sizable progressive patterns in customary exchange and the need for non-public statistics to skip global outskirts featured the need to diagram protection pointers and inspire particular guidelines to improve the nicely-being of residents' close to home statistics. A modern jump beforehand, which makes stressful situations to the well-being of individual records, is Cloud Computing. the rule of thumb highlight of Cloud Computing is that it allows on-name to arrange to get admission to figuring property with least control assignment or company association collaboration. This innovation gives new measurements to traditional exchanges of private records and due to this, it has become easy to installed order a safety affiliation for Cloud Computing administrations. For the easy out of the plastic new age of Cloud Computing, the idea device of a fitness inclusion is to shield humans and data, set proposals for foreseen conduct with the valuable asset of customers, problem threats and help to tune consistency with guideline This investigations paper centered at the development of a Cloud safety inclusion, in admire to facts insurance. focused on the model of programming as-a management (SaaS), this paper is meant to focus on a Framework for gatherings, clients, Cloud bearers and supply a gauge to the security inclusion of Cloud Computing. Pointed honestly on the protection requirements which is probably specific to Cloud circumstance, feature how those conditions connect to our Cloud well-being inclusion and endorse the measures, and the relating health regulations. except, it proposes a manner that might be observed with the manual of Cloud corporations for comparing the well-being in their structures as, insurance is one of the internal abilities of the cloud provide

Dr.K.Sai Manoj Proposed innovative Design and Development of Various Cloud Computing Architectures Improving the Security [17]-Numerous engineers have deliberate their very own format for introducing the distributed computing basis. The modern dispensed computing designs contrast from several points of view.

Protection has been the massive problem as patron related statistics and handling is embraced utilizing the framework gave by way of using outsider professional co-ops fluctuates especially. it's far vital to understand the degree of incorporation of security into the distributed computing framework and in some time discover the excellent layout that contains satisfactory and tight protection framework. in this examination paper, a correlation of present models from the factor of view of attention of protection foundation internal dispensed computing framework is added along with intensive engineering that is included with each a part of protection considering.

Dr.K.Sai Manoj Proposed Data Mining and Machine Learning Techniques for Cyber Security Intrusion Detection [18] - An interference discovery framework is customizing that screens a singular or an arrangement of PCs for toxic activities that are away for taking or blue-penciling information or spoiling framework shows. The most methodology used as a piece of the present interference recognition framework is not prepared to deal with the dynamic and complex nature of computerized attacks on PC frameworks. Despite the way that compelling adaptable methodologies like various frameworks of AI can realize higher discovery rates, cut down bogus alert rates, and reasonable estimation and correspondence cost. The use of data mining can realize ceaseless model mining, request, gathering, and littler than ordinary data stream. This examination paper portrays a connected with composing audit of AI and data delving procedures for advanced examination in the assistance of interference discovery. In perspective on the number of references or the congruity of a rising methodology, papers addressing each procedure were recognized, examined, and compacted. Since data is so fundamental in AI and data mining draws near, some striking advanced educational records used as a piece of AI and data burrowing are depicted for computerized security is shown, and a couple of recommendations on when to use a given system are given.

Dr.K.Sai Manoj active research [19] on Blockchain Cyber Security Vulnerabilities and Potential Countermeasures - Blockchain technology has attracted appreciable attention as a result of its big selection of possible application and it initial appear since a cryptocurrency, referred to as Bitcoin, however, have as be employed inside several different industry and non-business applications. In contrast to the majority presented the system to be supported decentralized system; this innovative expertise utilizes peer to peer networks and circulated a system which incorporates blockchain register to stock up connections. Its construction is intended as a digital log file and holds on as a series of coupled teams, referred to as blocks. Every individual block is latched cryptographically with the previous block. Once a block has been another, it can't be altered. Several security specialists speculate that the inherent cryptographically nature of the blockchain system is comfortable to resist constant hacking and security threats. However, earlier studies on the security and confidentiality of blockchain technology include given away that several applications contain fall casualty to thriving cyber-attacks. As a result of the growing require for cryptocurrency and its current security challenges, earlier study haven't centered on blockchain technology cybersecurity vulnerabilities extensively, and we study after to provide an additional way to spotlight potential attacks against blockchain technology weakness to cybersecurity

. Dr.K.Sai Manoj technically pointed on the [20] CHALLENGING ISSUES RELATED TO SOME SPECIFIC IMPORTANT PROBLEMS IN THE CLOUD PLATFORM- Load balancing in a cloud platform is one of the challenging issues and related to specific problems. Hence, generalized solutions for improving load balancing schemes in terms of time and cost are the need of the hour. Similarly, customized information delivery in real-time is another challenging issue in this computing environment. The development of an efficient algorithm is a requirement for content-based event dissemination in the pub/subsystem. Further integration of the sensor network with cloud computing has been investigated recently and has the opportunity to be integrated upon. There are many issues associated with deployment.

Dr.K.Sai Manoj proposed [21] Conceptual Oriented Analysis On the Industrial Standard Cyber Security- Digital computers have been chosen as a safety system in newly constructed nuclear facilities. Owing to digitalization, cyber threats to nuclear facilities have increased and the Integrity of the digital safety systems has been threatened. To cope with such threats, the nuclear regulatory agency has published guidelines for digital safety systems. This paper suggests an implementation method of cybersecurity for the safety system in the development phase. It introduces specific security activities based on a practice in a nuclear facility construction project. It also explains experiences resolving security vulnerabilities of the system and gives lessons learned about considerations in real construction.

Dr.K.Sai Manoj proposed [22] CONCEPTUAL ORIENTED ANALYSIS ON THE IMPACT ON THE CLOUD SECURITY ON THE CYBER ATTACKS- Many Developers are concentrating on research related to the cloud security techniques and measures have been intended to safeguard the cloud but cloud security is at high risk due to the innovative hacking techniques. This research paper addresses cloud security regarding three aspects to conclude the guidelines for improved cloud security. This research follows a three-layered research approach whereas each layer's outcome is directly affecting the investigations into the subsequent layers. At first, the structure and mechanism of the cloud security measures will be explored, for example, the use of firewalls, private cloud, encryption/decryption algorithms, digital signatures, and the protection against DOS attacks.

Dr.K.Sai Manoj Proposed [23] INVESTIGATIONS ON THE CLOUD DATA STORAGE SECURITY BASED USING DIFFIE HELLMAN ALGORITHM - This research mainly point out on the two data security concerns. On one hand, we focus on data confidentiality preservation which becomes more complex with flexible data sharing among a dynamic group of users. It requires the secrecy of outsourced data and an efficient sharing of decrypting keys between different authorized users. For this purpose, we, first, proposed a new method relying on the use of ID-Based Cryptography (IBC), where each client acts as a Private Key Generator (PKG). That is, we investigated on the own public elements and also investigated the corresponding private key using a secret. Second, we define CloudaSec, a public key-based solution, which proposes the separation of subscription-based key management and confidentiality-oriented asymmetric encryption policies. That is, CloudaSec enables flexible and scalable deployment of the solution as well as strong security guarantees for outsourced data in cloud servers. Expectation regarding experimental results, under Open Stack Swift, about the efficiency of CloudaSec in scalable data sharing, while considering the impact of the cryptographic operations at the client-side.

Dr.K.Sai Manoj Proposed [24] Analysis of the Technique for the Improvement of the Data Confidentiality in the Cloud Computing Environment -

Many Developers have been reviewed with some proposed solutions but these solutions have fallen short of addressing account misused and malicious insider threats. Besides, the online survey conducted highlighted that insider breaches are among the main form of vulnerability to cloud data. These challenges within the cloud storage informed the basis for the design of a scheme for improving data confidentiality in the cloud computing environment. The data confidentiality is achieved by implementing authentication login which triggers a six-digit code to be sent to a client mobile or e-mail for further authentication, thus, enabling situational awareness of data breaches in real-time. This approach will enhance the reliability and trust of cloud services enabling users to maximize potential benefits offered by the cloud environment

Dr.K. Sai Manoj Proposed [25] - Conceptual oriented analysis on the modern tools and techniques to Enrich Security Vulnerabilities in Ethical Hacking- The state of security on the internet is bad and getting worse. One reaction to this state of affairs is termed as Ethical Hacking which attempts to increase security protection by identifying and patching known security vulnerabilities on systems owned by other parties. As public and private organizations migrate more of their critical functions to the Internet, criminals have more opportunity and incentive to gain access to sensitive information through the Web application. Thus, the need of protecting the systems from the trouble of hacking generated by the hackers is to promote the persons who will punch back the illegal attacks on our computer systems. So, Ethical hacking is an assessment to test and check an information technology environment for possible weak links and vulnerabilities. Ethical hacking describes the process of hacking a network ethically, therefore with good intentions. This research paper describes what ethical hacking is, what it can do, and ethical hacking methodology as well as some tools which can be used for an ethical hack.

Dr.K.Sai Manoj Proposed [26] Investigation on Cloud Computing in terms of the current trends and also to meet_the important challenges with security for the improvement of the Health care services- Cloud computing is a new challenge in terms of the delivering computing resources and services. Many developer's and expert's expectations are that it can improve health care services, a lot of benefits in health care research, and also tremendous change in the technology of health information. However, as with any type of new investigation, cloud computing should be carefully evaluated before proposing to the new idea. This paper investigates the conceptually oriented research in health care and applies on the two stages such as technology and security to investigate the new challenges of this computing model.

Dr.K. Sai Manoj proposed [27] Investigation on the security aspects of cloud computing using symmetric and asymmetric algorithms - Many Developers are concentrating on the security aspect of cloud computing. Still, there is a need to concentrate on the investigation of the new type of security algorithms. In this research paper, we had done an investigation on the comparison of symmetric and asymmetric algorithms. Data security is one of the very important issues in cloud computing. In this article, we investigated the comparative study on one important technique related to the symmetric and asymmetric algorithm that enhanced Data Security in the cloud computing system. We Pointed AES for symmetric encryption algorithm and Elliptic curve for the asymmetric encryption algorithm.

Dr.K.Sai Manoj proposed [28] Investigation on the Attribute-Based Encryption for Secure Data Access in Cloud - Cloud computing is a progressive computing worldview, which empowers adaptable, on request, and ease use of Information Technology assets. However, the information transmitted to some cloud servers, and various protection concerns are arising out of it. Different plans given the property-based encryption have been proposed to secure the Cloud Storage. In any case, most work spotlights on the information substance security and the get to control, while less consideration towards the benefits control and the character protection. In this paper, a semi-anonymous benefit control conspires AnonyControl to address the information protection, as well as the client character security in existing access control plans. AnonyControl decentralizes the central authority to restrain the character spillage and accordingly accomplishes semi-anonymity. Furthermore, it likewise sums up the document to get to control the benefits control, by which advantages of all operations on the cloud information managed in a fine-grained way. Along these lines, display the AnonyControl-F, which ultimately keeps the character spillage and accomplish the full secrecy. Our security assessment demonstrates that both AnonyControl and AnonyControl-F are secure under the decisional bilinear Diffie-Hellman presumption, and our execution assessment shows the attainability of our plans.

Dr.K.Sai Manoj proposed [29] INVESTIGATION ON THE DATA SECURITY IN CLOUD COMPUTING USING BIOMETRICS - With the rapid increase in the usage of cloud computing, it is very important to address the security issues also. Many Developers are designing so many techniques. Still, there are some problems related to authentication in the cloud environment. In cloud comp data and software are fully not contained on the user's computer; Data Security concerns arising because both user data and program are residing in Provider Premises. Clouds typically have single security architecture but have many customers wi demands. Every cloud provider solves this problem by encrypting the data by using encryption algorithms. This research paper Point out clearly on such problems and their solution with the use of Biometric techniques.

Dr.K.Sai Manoj proposed [30] Research on Security and Vulnerabilities of Blockchain Systems- Recent research successfully improved the unauthorized access to data in a system pointing clearly on the blockchain technology and also hack from these systems have raised more restrictions about whether this new technology can be secured from ongoing, evolving cyber-attacks. While the technology is known to provide an environment that is fundamentally safer than other existing centralized systems offer, security professionals, warn that the current blockchain ecosystem is still technically not fully developed and also so much of investigations are required, technology needs to improve for many known as well as unknown imperfection [1]. This research paper focused upon the number of research studies and various other technology-related things pointing to blockchain systems security.

Dr.K.Sai Manoj proposed [31] Conceptual Oriented Analysis on the security based on the SaaS Cloud Computing Architecture for the Cyber Security Issues - The Main aim of this research paper is to focus on the extensive literature survey to analyze the concept of the user-oriented cybersecurity and also to point out that concept on the cloud computing architecture as a SaaS. Cloud infrastructure is closely related to its architecture and comprises of many cloud components. In this research paper, we proposed a cloud computing-based architecture for facing cybersecurity situation awareness. Especially; we pointed out the cloud computing security architecture for SaaS with a reduction of the cost for data storage and also to investigate the efficient stream processing techniques to reduce operational delays. The main important thing is to detect threats; we pointed out a parallel cloud-based threat detection that integrates both signature-based detection and anomaly-based detection

Dr.K.Sai Manoj proposed [32] Investigation On The Cloud Computing Security Using PET and REMOTE Attestation in Cloud Architectures. Cloud computing offers opportunities for organizations to reduce IT costs by using the computation and storage of a remote provider. Despite the benefits offered by the cloud computing paradigm, organizations are still wary of delegating their computation and storage to a cloud service provider due to trust concerns. The trust issues with the cloud can be addressed by a combination of regulatory frameworks and supporting technologies. Privacy Enhancing Technologies (PET) and remote attestation provide the technologies for addressing trust concerns.

Dr.K.Sai Manoj proposed [33] Investigation on the Data Protection in the cloud using Predicate Based Encryption This Research investigates how Predicate Based Encryption (PBE) could be leveraged within the cloud to protect data. PBE is a novel family of asymmetric encryption schemes in which decryption of a ciphertext is dependent upon a set of attributes satisfying a certain predicate, allowing for selective grained access control to be specified over cipher-texts. It is argued that the obfuscation of one's data is not enough when seeking to protect data. The control of how one's data is used and the trust an order to service providers is equally as important. To this end, three archetypal scenarios are described that illustrate ways in which service users could specify precisely with whom they wish to share their data, for what purpose, and for how long. Furthermore, two additional scenarios are presented that would allow a service provider to facilitate keyword search over encrypted data using expressive queries supporting conjunction and disjunction of terms.

Dr.K.Sai Manoj proposed [34] A Survey on Protection of Multimedia Content in Cloud Computing. In this Modern Online World Security Plays an Important role. Cloud Computing algorithms have the Capability to Disable Privacy. Multi-Media is the Clear Integration of data, text, image, audio, video in one application. In this Paper We Introduced Algorithm with Good Concept to Protect 2-D Videos, 3-D

Videos, Audio, and Image. This new type of Cloud Computing system detects Duplicate and Copyrighted material in the Online.

Dr.K.Sai Manoj proposed [35] UNCRACKABLE CIPHER DYNAMIC DOUBLE ENCRYPTION STANDARD IN CLOUD FOR DATA ACCESS CONTROL AND PRIVACY PRESERVING MECHANISM - Nowadays, the excessive use of internet cloud has received much attention. Cloud computing is the evolving paradigm that provides the services in which cloud consumers can remotely store their data into the cloud and access the on-demand high-quality applications. Cloud computing is mainly used for resource sharing and with very low-maintenance. In the existing Extendable Access Control System procedure, the authority is the trusted party, but in many cases, they may perform an illegal action which leads to data loss. In the proposed work encryption of data is done through Uncrackable Cipher Dynamic Double Encryption Standard (UCDDES). UCDDES performs with the key length of 32, 40, and 48. After dynamically selecting the key length the data governor sent the key request to the authority. Then the data governor generates the partial secret key based on the obtained key length. It is further used to decrypt the data and store it in the cloud. As a result, the security of cloud and access control is improved and the problems faced by the unauthorized users/ hackers accessing data are reduced. It also increased cloud security and prevented from dictionary attacks, brute force attacks, collision attacks, and so on. Nowadays, the excessive use of the internet cloud has received much attention. Cloud computing is the evolving paradigm that provides the services in which cloud consumers can remotely store their data into the cloud and access the on-demand high-quality applications. Cloud computing is mainly used for resource sharing and with very low-maintenance. In the existing Extendable Access Control System procedure, the authority is the trusted party, but in many cases, they may perform an illegal action which leads to data loss. In the proposed work encryption of data is done through Uncrackable Cipher Dynamic Double Encryption Standard (UCDDES). UCDDES performs with the key length of 32, 40, and 48. After dynamically selecting the key length the data governor sent the key request to the authority. Then the data governor generates the partial secret key based on the obtained key length. It is further used to decrypt the data and store it in the cloud. As a result, the security of cloud and access control is improved and the problems faced by the unauthorized users/ hackers accessing data are reduced.

It also increased cloud security and prevented from dictionary attacks, brute force attacks, collision attacks, and so on.

Dr.K.Sai Manoj proposed [36**] Faster content sharing over the smartphone-based** Delay- tolerant networks -Delay Tolerant Network (DTN) service and protocol stack and presents an implementation of it on the Android platform that is called "Bytewalla". It allows the use of Android phones for the physical transport of data between network nodes in areas where there are no other links available, or where existing links need to be avoided for security reasons or in case the Internet is shut down by a government authority as it happened in some Arab countries during the spring of 2011. With the growing number of smartphone users, peer-to-peer ad hoc content sharing is expected to occur more often. Thus, new content sharing mechanisms should be developed as traditional data delivery schemes are not efficient for content sharing due to the sporadic connectivity between smartphones. To accomplish data delivery in such challenging environments, researchers have proposed the use of store-carryforward protocols, in which a node stores a message and carries it until a forwarding opportunity arises through an encounter with other nodes. Most previous works in this field have focused on the prediction of whether two nodes would encounter each other, without considering the place and time of the encounter. In this paper, we propose discover-predict-deliver as an efficient content sharing scheme for delay-tolerant smartphone networks. In our proposed scheme, contents are shared using the mobility information of individuals. Specifically, our approach employs a mobility learning algorithm to identify places indoors and outdoors. A hidden Markov model is used to predict an individual's future mobility information. Evaluation based on real traces indicates that with the proposed approach, 87 percent of contents can be correctly discovered and delivered within 2 hours when the content is available only in 30 percent of nodes in the network. We implement a sample application on commercial smartphones, and we validate its efficiency to analyze the practical feasibility of the content sharing application. Our system approximately results in a 2 percent CPU overhead and reduces the battery lifetime of a Smartphone by 15 percent at most. The implementation of a store and forward messaging application and a Sentinel Surveillance health-care application (SSA) that runs on top of Bytewalla are presented together with a few usage scenarios. We conclude that the integration of DTN links in the general IP-network architecture on the mobile phone platform is feasible and will make it easier to integrate DTN applications into communication-challenged areas. To our knowledge, our implementation of the bundle protocol is the first on the Android platform.

Buyya et al. proposed [37] investigations on the present technology based on the security pointing to cloud computing. This author done a broad study on the cloud and also done a huge investigation pointing to risk factors and security challenges in software as a Service (SaaS) model of cloud computing and also mentioned technically future challenges on cloud computing.

Dr.K.Sai Manoj proposed [38] A Study on Data Controller-Preserving Public Auditing for Secure Cloud Storage- While cloud computing makes these advantages more appealing than ever, it also brings new and challenging security threats toward users' outsourced data. Since cloud service providers (CSP) are separate administrative entities, data outsourcing is relinquishing user's ultimate control over the fate of their data

Dr.K.Sai Manoj proposed [39] A Dynamic Framework of Advanced Mobile Video Streaming and Social video sharing in clouds- The media data has grown over years in all streams of technology. Video and images play a vital role in communication around the globe. The usage of the mobile device along with media has boomed the year age of technology. The usage of traditional networking and service providers lacks to provide the quality-centered and reliable service to the mobile users concerning with the media data. The vital problems that lead to the poor services from the service providers would be low bandwidth which affects the efficient transfer of video to the user, the disruption of video streaming also occurs due to the low bandwidth. The buffer time of the video over mobile devices which moves from place to place affects the smooth streaming and also sharing of video from one user to another user over social media. Our survey shows the functioning of various methods and architecture which used the cloud to provide an effective solution for providing better service to the users. AMES is cloud architecture built specially to provide video service to the user. The study has come up with an optimal solution, proposing with a video cloud, which collects the video from video service providers, and providing reliable service to the user. While demands on video traffic over mobile networks have been souring, the wireless link capacity cannot keep up with the traffic demand. The gap between the traffic demand and the link capacity, along with time-varying link conditions, results in poor service quality of video streaming over mobile networks such as long buffering time and intermittent disruptions. Leveraging the cloud computing technology, we propose a new mobile video streaming framework, dubbed AMES-Cloud, which has two main parts: AMV (adaptive mobile video streaming) and ESV (efficient social video sharing). AMV and ESV construct a private agent to provide video streaming services efficiently for each mobile user. For a given user, AMV lets her private agent adaptively adjust her streaming flow with a scalable video coding technique based on the feedback of link quality. Likewise, ESV monitors the social network interactions among mobile users, and their private agents try to prefetch video content in advance. We implement a prototype of the AMES-Cloud framework to demonstrate its performance. It is shown that the private agents in the clouds can effectively provide adaptive streaming, and perform video sharing (i.e., prefetching) based on the social network analysis.

Dr.K.Sai Manoj proposed [40] Faster content sharing over the Smartphone-based Delay- tolerant networks - Delay Tolerant Network (DTN) service and protocol stack and presents an implementation of it on the Android platform that is called "Bytewalla". It allows the use of Android phones for the physical transport of data between network nodes in areas where there are no other links available, or where existing links need to be avoided for security reasons or in case the Internet is shut down by a government authority as it happened in some Arab countries during the spring of 2011. With the growing number of Smartphone users, peer-to-peer ad hoc content sharing is expected to occur more often. Thus, new content sharing mechanisms should be developed as traditional data delivery schemes are not efficient for content sharing due to the sporadic connectivity between smart phones. To accomplish data delivery in such challenging environments, researchers have proposed the use of store-carry-forward protocols, in which a node stores a message and carries it until a forwarding opportunity arises through an encounter with other nodes. Most previous works in this field have focused on the prediction of whether two nodes would encounter each other, without considering the place and time of the encounter. In this paper, we propose discover-predict-deliver as an efficient content sharing scheme for delay-tolerant Smartphone networks. In our proposed scheme, contents are shared using the mobility information of individuals. Specifically, our approach employs a mobility learning algorithm to identify places indoors and outdoors. A hidden Markov model is used to predict an individual's future mobility information. Evaluation based on real traces indicates that with the proposed approach, 87 percent of contents can be correctly discovered and delivered within 2 hours when the content is available only in 30 percent of nodes in the network. We implement a sample application on commercial smartphones, and we validate its efficiency to analyze the practical feasibility of the content sharing application. Our system approximately results in a 2 percent CPU overhead and reduces the battery lifetime of a Smartphone by 15 percent at most. The implementation of a store and forward messaging application and a Sentinel Surveillance health-care application (SSA) that runs on top of Bytewalla are presented together with a few usage scenarios. We conclude that the integration of DTN links in the general IP-network architecture on the mobile phone platform is feasible and will make it easier to integrate DTN applications into communication-challenged areas. To our knowledge, our implementation of the bundle protocol is the first on the Android platform

Dr.K.Sai Manoj proposed [41] An Efficient and Novel Approach Using T.H.E.S Methodology for CBIR - the search engine is expected to extract results with the high-end accuracy. The basic motto behind the image search engines is no different. It should retrieve the best possible match from the database for the query made. But, the accessible search engines are based on the keywords only. To overcome the inefficiencies in this approach, we are proposing a search based on CBIR (content-based image retrieval). This paper discusses, in-depth, about the methodologies to construct an efficient CBIR and also presents a novel approach that performs with increased efficiency in many aspects. We have used Open CV, an image processing toolbox for implementing and testing our concepts. We present a query formulation language (called Mash QL) to easily query and fuse structured data on the web. The main novelty of Mash QL is that it allows people with limited IT skills to explore and query one (or multiple) data sources without prior knowledge about the schema, structure, vocabulary, or any technical details of these sources. More importantly, to be robust and cover most cases in practice, we do not assume that a data source should have—an offline or inline—schema. This poses several language-design and performance complexities that we fundamentally tackle.

CYBERSECURITY CHALLENGES IN LITERATURE SURVEY

These are the points addressed in various cybersecurity proposals and analysis the challenges have been outlined below;

- Few Concepts have been implemented with the service security license which maintains the security platform and since the service industry should not maintain all the security infrastructure due to the costing involved behind.
- Other topics also concentrated on secure data Confidentiality without considering Cloud account Integrity, unrestricted, and authorization.
- Few of the proposals were fully written in theoretical instead of practical implementation and there will not any results related to this proposal.
- In some papers, though the Cyber data security technique proposed seams reliable, it looks expensive, real-time implement complication, and hard to understand.
- Few security proposal techniques are not experimentally verified like the Data Access Control and Secure Data Confidentiality (DACSDC)

Conclusion Based on the Literature survey

Mobile Cloud Computing is the dynamic cloud data services; cloud edge servers, Cloud data storage, Online databases, Cloud edge networking, System access software, data analytics, system intelligence, and finally high data connection to provide free access and create the opportunity, Easy access resources, and small budget economies. Mobile Cloud computing is an emerging social phenomenon that is been patronize by individuals almost every day. At most any upcoming technology, it does create new problems and affects the function of the system and now the mobile cloud computing is developed in all the way to decrease the manual involvement in supplies and management by using this concept we will provide more productivity with the help of modern hardware and software virtualization.

The phenomenon of Cloud Computing is very promising which ensures businesses increase efficiency alongside reducing their cost of production. Data protection and security in cloud computing are still crawling on its knees and need more research attention although it has been deployed and used in the production environment.

Data Security in Cloud Computing is an important area that should be given much attention. A large amount of data these days circulate in the cloud which has given room for intruders and eavesdroppers to try and get hold of them. It is therefore essential, for vigorous study on how to propose and implement a robust and functioning security mechanism that will prevent hackers from getting access to the data being transmitted to and fro in the cloud.

Based on the information presented in this study, through the analysis of various papers and the insight gotten from the implementation of the proposed techniques, it is realized that majority of the papers give much attention to data confidentiality whilst few papers satisfy the three aspects of security; Confidentiality, Integrity, and Availability.

References:

1. Muijnck-Hughes Jan de (2011) *Data Protection in the cloud,* 12 Jan 2019 [Online], Available: http://www.ru.nl/ds
2. Venkata S. et.al (2011) *Security Techniques for Protecting Data in Cloud Computing*, 12 Jan 2019 [Online] Available: https://www.bth.se/com
3. Ali Asghary K. (2011) *Security Analysis and Framework of Cloud Computing with Parity-Based Partially Distributed File System*, 26, Jan 2019 [Online] Available; https://www.academia.edu/27767213/security_Analysis_and_Framework_of_cloud_computing_with_Parity_Based_Partially_Distributed_File_System
4. Nabil Giweli (2013) *Enhancing Cloud Computing Security and Privacy*, 20, Jan 2019 [Online]Available:https://www.researchdirect.westernsydney.edu.au/islandora/object/uws%3AI7310/.../view
5. Zhou Miao (2013)*Data Security and Integrity in cloud computing*, Doctor of Philosophy thesis, School of Computer Science and Software Engineering, University of Wollongong. http://www.ro.uow.edu.au/thesis/3990
6. Sudhansu R. L. et.al *Enhancing Data Security in Cloud Computing Using RSA Encryption and MD5 Algorithm*, International Journal of Computer Science Trends and Technology (IJCST) – Volume 2, Issue 3, June 2014

7. Aastha Mishra (2014) *Data Security in Cloud Computing Based on Advanced Secret Sharing Key Management System*, 20 Jan 2019 [Online] Available: https://www.ethesis.nitrkl.ac.in/5845/1/212CS2110.pdf
8. NesrineKaaniche (2014) *Cloud Data Security based on Cryptographic Mechanisms*, 26 Jan 2019 [Online] Available: https://www.tel.archives-ouvertes.fr/tel-01146029/document
9. Afnan U.K. (2014) Data Confidentiality and Risk Management in Cloud Computing 2 Feb 2019 [Online]Available:https://www.ethesis.whiterose.ac.uk/13677/1/Thesis_Final_Afnan_27072016_EngD.pdf
10. Sarojini G. et.al (2016) Trusted and Reputed Services using Enhanced Mutual Trusted and Reputed Access Control Algorithm in Cloud, 2nd International Conference on Intelligent Computing, Communication & Convergence (ICCC-2016). www.sciencedirect.com
11. Dimitra A. G. (2017) Security Policies for Cloud Computing, 26 Jan 2019 [Online] Available: https://www.dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/11007/Georgiou_Dimitra.pdf?
12. **Conceptual oriented study on the cloud computing architecture for the full-security**, Dr.K.Sai Manoj International Journal of Engineering & Technology, Science Publishing Corporation **(SPC)** https://www.sciencepubco.com/index.php/ijet/article/view/11654
13. Cloud security: risk factors and security issues in current trends Dr.K.SaiManoj International Journal of Engineering & Technology, Science Publishing Corporation October 2019 (Scopus) (Single Author) https://www.sciencepubco.com/index.php/ijet/issue/view/495 (Indexed in German National Serials Database (ZDB) (Germany), ProQuest (USA), etc)
14. Risk Factors And Security Issues In Various Cloud Storage Operations Dr.K.Sai Manoj Volume-8 Issue-12, October 2019, ISSN: 2278-3075 (Online) Published By Blue Eyes Intelligence Engineering & Sciences Publication
15. Conceptually based on the Data Mining Techniques for the Prediction of Hydration Assessment, Breath Analysis and Heart Disease International Journal of Innovative Technology and Exploring Engineering (IJITEE) Dr.K.Sai Manoj ISSN: 2278-3075, Volume-8 Issue-12S2, October 2019

http://www.ijitee.org/wp-content/uploads/papers/v8i12S2/L107510812S219.pdf

16. Research on the Security Policies for Cloud Computing International Journal of Innovative Technology and Exploring Engineering (IJITEE) Dr.K.Sai Manoj ISSN: 2278-3075, Volume-8 Issue-12S2, October 2019 http://www.ijitee.org/wp-content/uploads/papers/v8i12S2/L107610812S219.pdf
17. Design and Development of Various Cloud Computing Architectures Improving the Security International Journal of Innovative Technology and Exploring Engineering (IJITEE) Dr.K.Sai Manoj ISSN: 2278-3075, Volume-8 Issue-12S2, October 2019
18. Data Mining and Machine Learning Techniques for Cyber Security Intrusion Detection International Journal of Engineering and Advanced Technology (IJEAT) Dr.K.Sai Manoj Dr.P.S.Aithal ISSN: 2249 – 8958, Volume-9 Issue-3, February 2020 https://www.ijeat.org/download/volume-9-issue-3/
19. Blockchain Cyber Security Vulnerabilities and Potential Countermeasures International Journal of Innovative Technology and Exploring Engineering (IJITEE) Dr.K.Sai Manoj Dr.P.S.Aithal ISSN: 2278-3075, Volume-9 Issue-5, March 2020 http://www.ijitee.org/wp-content/uploads/papers/v9i5/E2170039520.pdf
20. CHALLENGING ISSUES RELATED TO SOME SPECIFIC IMPORTANT PROBLEMS IN THE CLOUD PLATFORM by Dr.K.Sai Manoj published in the merit list by International Journal of Computer Engineering and Applications Volume XIII, Issue VIII JAN 2020. (UGC Approved Journal with Thomson researcher id) (Single author)
21. Conceptual Oriented Analysis On The Industrial Standard Cyber Security by Dr.K.Sai Manoj published in International Journal of Computer Science Trends and Technology (IJCST) – Volume 7 Issue 4, Jul - Aug 2019 (**Single Author)** http://www.ijcstjournal.org/volume-7/issue-4/IJCST-V7I4P3.pdf
22. CONCEPTUAL ORIENTED ANALYSIS ON THE IMPACT ON THE CLOUD SECURITY ON THE CYBER ATTACKS by Dr.K.Sai Manoj selected in the merit list by Journal of Analysis and Computation (JAC) (An International Peer Reviewed Journal), www.ijaconline.com, ISSN 0973-2861 Volume XII, Issue I, May 2019 (First Author)

http://www.ijaconline.com/conceptual-oriented-analysis-impact-cloud-security-cyber-attacks/

23. INVESTIGATIONS ON THE CLOUD DATA STORAGE SECURITY BASED USING DIFFIE HELLMAN ALGORITHM by Dr.K.Sai Manoj selected in the merit list by International Journal of Computer Engineering and Applications, Volume XIII, Issue VI, JUNE. 19, www.ijcea.com ISSN 2321-3469 (First Author) http://www.ijcea.com/investigations-cloud-data-storage-security-based-using-diffie-hellman-algorithm/
24. Analysis of the Technique for the Improvement of the Data Confidentiality in the Cloud Computing Environment by Dr.K.Sai Manoj Published in International Journal of Computer Science Trends and Technology (IJCST) – Volume 7 Issue 4, Jul - Aug 2019 **(First Author)** http://www.ijcstjournal.org/volume-7/issue-4/IJCST-V7I4P5.pdf
25. Conceptual oriented analysis on the modern tools and techniques to Enrich Security Vulnerabilities in Ethical Hacking Dr.K.Sai Manoj International Journal of Computer Science Trends and Technology (IJCST) in May-June 2019, Volume Number 7 Issue3 with ISSN: 2347-8578 & ISO 3297:2007.This Journal has Thomson Reuters ResearcherID: M-3066-2016. **(First Author)** http://www.ijcstjournal.org/volume-7/issue-3/IJCST-V7I3P25.pdf
26. Investigation on the Cloud Computing in terms of the current trends and also to meet_the important challenges with security for the improvement of the Health care services Dr.K.Sai Manoj IJCEA Feb. 2019, with Thomson Reuters Research Id: P1671-2016. Also, It is UGC approved Journal. For this article author Dr.K.Sai Manoj research article in the merit list from the Reviewers and Editorial Team. **(First Author)** http://www.ijcea.com/investigation-cloud-computing-terms-current-trends-also-meet-important-challenges-security-improvement-health-care-services/
27. Investigation on the security aspects of cloud computing using symmetric and asymmetric algorithms, Dr.K.Sai Manoj International Journal of Computer Engineering and Applications, Volume XIII, Issue I, January. 19, www.ijcea.com ISSN 2321-3469 with Thomson Reuters Research Id: P1671-2016. Also, It is UGC approved Journal. For this article author Dr.K.Sai Manoj received an appreciation certificate in the merit list from the Editor.

(**First Author)** http://www.ijcea.com/investigation-security-aspects-cloud-computing-using-symmetric-asymmetric-algorithms/

28. Investigation on the Attribute-Based Encryption for Secure Data Access in Cloud, Dr.K.Sai Manoj International Journal of Computer Science Trends and Technology (IJCST) with Thomson Reuters Researcher ID: M-3066-2016 – Volume 6 Issue 6, Nov-Dec 2018. ISSN: 2347-8578 (**First Author)** https://www.scribd.com/document/393639933/IJCST-V6I6P13-Dr-K-SAI-MANOJ-Ms-K-Mrudula-Mrs-K-Maanasa-K-Phani-Srinivas
29. INVESTIGATION ON THE DATA SECURITY IN CLOUD COMPUTING USING BIOMETRICS International journal of current advanced research UGC approved and also Thomson Reuters journal with researcher id and END NOTE ISSN: O: 2319-6475, ISSN: P: 2319-65,Impact factor:6.614, Volume 7;Issue 12(B);December 2018;Page No.16473-16475.(**First Author)** http://journalijcar.org/issues/investigation-data-security-cloud-computing-using-biometrics
30. Research on Security and Vulnerabilities of Blockchain Systems by Dr.K.Sai Manoj published in International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177 Volume 8 Issue I, Jan 2020 (Single Author) https://www.ijraset.com/fileserve.php?FID=26233
31. Conceptual Oriented Analysis on the Security based on the SaaS Cloud Computing Architecture for the Cyber Security Issues by Dr.K.Sai Manoj published in International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177 Volume 7 Issue VII, July 2019 (**First Author)** https://www.ijraset.com/fileserve.php?FID=24254
32. INVESTIGATION ON THE ON THE CLOUD COMPUTING SECURITY USING PET AND REMOTE ATTESTATION IN CLOUD ARCHITECTURES by Dr.K.Sai Manoj published in International Journal of Current Advanced Research Volume 8; Issue 10 (D); October 2019 http://dx.doi.org/10.24327/ijcar.2019 Impact Factor: 6.614 ISSN: O: 2319-6475, ISSN: P: 2319-6505; October 2019 http://journalijcar.org/issues/investigation-cloud-computing-security-using-pet-and-remote-attestation-cloud-architectures

33. Investigation on the Data Protection in the Cloud using Predicate Based Encryption International Journal of Computer Science and Information Technology Research UGC approved with ISSN 2348-120X (Online) Vol. 6, Issue 4, pp: (61-65), Month: October - December 2018. (**First Author)** http://www.researchpublish.com/journal/IJCSITR/Issue-4-October-2018-December-2018/0

34. A Survey on Protection of Multimedia Content in Cloud Computing, Dr. K.Sai Manoj, Mrudula Kudaravalli, International Journal of Computer Science and Mobile Computing - Vol.6 Issue.11, November- 2017, pg. 7-11 (**First Author**) http://ijcsmc.com/docs/papers/November2017/V6I11201705.pdf

35. UNCRACKABLE CIPHER DYNAMIC DOUBLE ENCRYPTION STANDARD IN CLOUD FOR DATA ACCESS CONTROL AND PRIVACY PRESERVING MECHANISM Dr. K. Sai Manoj, World Journal of Engineering Research and Technology WJERT 2019, Vol. 5, Issue 6, 437-45 (First Author) https://www.wjert.org/admin/assets/article_issue/35102019/1575371428.pdf

36. **Faster content sharing over the smartphone**-based Delay- tolerant networks. Dr. Sai Manoj Kudaravalli, International Journal of Engineering Research- Online. Vol.5,Issue.4,2017,ISSN: 2321-7758. July-Aug. Article available online http://www.ijor.in;

37. Buyya, R., Broberg, J., & Goscinski, A. (2011). Cloud Computing: Principles and Paradigms. Cloud Computing: Principles and Paradigms. New Jersey: John Wiley & Sons, Inc. https://doi.org/10.1002/9780470940105

38. A Study on Data Controller-Preserving Public Auditing for Secure Cloud Storage, Dr. K. Sai Manoj, International Journal of Modern Engineering Research (**First Author**) http://www.ijmer.com/pages/Vol.8-Iss.1(Version-1).html

39. **A Dynamic Framework** of Advanced Mobile Video Streaming and Social video sharing in clouds, Dr. Sai Manoj Kudaravalli, International Journal of Engineering Research Online. Vol.5., Issue.5,2017, sept-oct, ISSN:23217758.With an Impact Factor 5.8701, Article available online http://www.ijoer.in.

40. **Faster content sharing over the smart phone**-based Delay- tolerant networks. Dr. Sai Manoj Kudaravalli, International Journal of Engineering

Research- Online. Vol.5,Issue.4,2017,ISSN: 2321-7758. July-Aug. Article available online http://www.ijor.in;

41. An Efficient and Novel Approach Using T.H.E.S Methodology for CBIR, Dr. Sai Manoj Kudaravalli, International journal of computer science Mechatronics. SJIF-4.454|Vol.3.Issue .5.2017. ISSN: 2455-1910

Chapter 4

4 Chapter 4 : Related Work

Related work

CHALLENGES OBSERVED IN LITERATURE SURVEY

Few challenges or issues that were identified during reading and analysing the research papers have been outlined below; some of the research papers focused their implementation on Platform as a service and Software as a service leaving Infrastructure as a service behind.

Other papers also concentrated on data Confidentiality without taking into account Integrity, non-repudiation, and authenticity. Few of the papers were theoretical based meaning actual practical implementation was not done. In other papers, though the technique proposed seams reliable, but it looks weird, complicated, and cumbersome to implement. Some proposed techniques were also not experimentally validated like the Access Control and Data Confidentiality (ACDC)

4.1 Motivation and Research Objective:

Due to the increased demand in the multimedia content in which videos have the highest request factor of 78% traffic on the network until 2022 [7]. The huge demand of videos can create extensive traffic load and congestion on the network core and at backhaul which leads to the strategies and techniques that will deal with these problems, Mobile Cloud Computing ICN provides an in-networking caching mechanism that is a better way to handle these issues [10]. On the other hand 5G-Mobile Cloud Computing ICN architecture in [4] provides higher bandwidth to support higher quality video streaming which utilizes the (mmWave) techniques and also supports mobility. While 5G network can impose longer connection delays due to frequent handoff cause of shorter transmission range between base station which can degrade the QoE for mobile video users. Group mobility into 5G- Mobile Cloud Computing ICN architecture hasn't caught the attention of the researchers only individual nodes mobility has been taken in to count [4][9].

4.1.1 Research Objective:

Cloud Computing is the delivery of computing services; servers, storage, databases, networking, software, analytics, intelligence, and the internet to offer faster innovation, flexible resources, and economies of scale. Cloud computing is an emerging social phenomenon that is been patronized by individuals almost every day. For any important emerging technology, it comes with its issues that hinder its adoption. Currently, cloud computing is seen as a fast-developing area that can instantly supply extensible service by using the internet with the help of hardware and software virtualization.[12]

4.2 Investigation on the Data Protection in the Cloud using Predicate Based Encryption:

Cloud Computing is the name given to the recent trend in computing service provision. This trend has seen the technological and cultural shift of computing service provision from being provided locally to being provided remotely and en masse, by third-party service providers. Functionality such as storage, processing, and other functionality is now on-demand, as a service and both freely and at cost. Data that was once housed under the consumer's own administrative and security domain has now been extracted and placed under the domain of the Cloud Service Provider (CSP). The consumer has lost control over how their data is being stored, shared, and used, and also over the security used to protect their data. Moreover, it can be the case that a surreptitious employee of the service provider will have access to your data for legitimate purposes but will abuse this power for their means. Users are no longer in full control over the security of their data and the protection by the service provider is not absolute. There is a need for users to have more control over the protection of their data within the cloud: Users need to become empowered [1].

4.2.1 The investigation was divided broadly into three stages.

1) Data Security and the Cloud. The initial stage sought to provide a clear picture regarding Cloud Computing and the security issues therein, looking to identify precisely where and when threats can occur to data and how these threats ought to be mitigated.

2) Predicate Based Encryption. The next stage focused solely upon PBE schemes discussing how they work and what they allow for. This provided a foundation upon which their deployment as part of a crypto-system could be explored and to the types of problems that PBE schemes can be used to solve.

3) Leveraging PBE. The final stage of the investigation built upon and combined the results, of the previous stages. Here the investigation looked to determine the problems that PBE schemes can be used to solve within the Cloud, and the quality of the solution provided.

4.2.2 Research Outcomes:

From the investigation, it was determined that PBE can be used to protect data within the cloud. The main results for each stage of the investigation are outlined below. Data Security and the Cloud. From the initial stage, two threat-models were produced: one user and the other CSP orientated. These models described the threats upon data in terms of the data lifecycle. Furthermore, it was determined that a privacy model centered around Kafka's. The Trial together with the idea that the CSP provider could be trusted facilitates a better understanding of the problems present within the Cloud and how such problems can be solved. Predicate Based Encryption. Characteristics that can be used to categorize PBE schemes were identified. Of which predicate placement had the greatest act upon the access control by the scheme. A generic model for deploying PBE schemes as part of a crypto-system was developed. From this model three modes of operation that characterizes the deployment of a PBE scheme were identified. Leveraging Predicate Based Encryption. Three scenarios are described that illustrate ways in which service users could specify precisely with whom they wish to share their data, for what purpose, and for how long. Furthermore, two additional scenarios are presented that would allow a service provider to facilitate keyword search over encrypted data using expressive queries supporting conjunction and disjunction of terms.[2].

4.3 DATA SECURITY WITHIN THE CLOUD OVERVIEW:

Cloud Computing is the name given to a recent trend in computing service provision. This trend has seen the technological and cultural shift of computing service provision from being provided locally to being provided remotely and en masse, by third-party service providers. This new means of service provision has evolved from and is the culmination of research stemming from (among others) distributed and networked systems, utility computing, the web and software services research. This paradigm shift has led to computing being seen as another household utility and has prompted many a business and individual to migrate parts of their IT infrastructure to the cloud and for this data to become managed and hosted by Cloud Service Providers (CSPs). Computing as a Service: One of the main tenets of Cloud Computing is the `as-a-Service' paradigm in which `some' service by a Service Provider (also known as a Cloud Service Provider) to a User (consumer) for use. This service can also be categorized according to the application domain of its deployment. Examples of application domains that services are: Financial e.g. Mint.com, Managerial e.g. Ever Note and Analytical e.g. Google Analytics. The agreed terms of use, indicating the actions that must be taken by both the provider and consumer, are described in a contract that is agreed upon before service provision. Failure to honor this agreement can lead to denial of service for the consumer or legal liability for the service provider. This contract is often described as a Terms of Service or Service Level Agreement. Moreover, as part of this agreement the service provider will provide a Privacy Policy that outlines how the user's data will be stored, managed, used, and protected. Service Levels: Software as a Service: The highest layer is known as Software as a Service (SaaS). It represents the applications that are deployed/enabled over a cloud by CSPs. These are mature applications that often API to allow for greater application extensibility. For instance, Google Docs can be seen as the archetypal SaaS application, it has been deployed solely within the Cloud and several APIs to promote the use of the application. Platform as a Service: The next layer is known as: Platform as a Service (PaaS). This represents a development platform that developers can utilize to write, deploy, and manage applications that run on the cloud. This can include aspects such as development, administration and management tools, run-time and data management engines, and security and user management services. For instance, Force.com and Amazon Web Services [AWS] a suite of services that allows developers to construct an application that is deployed using web-based tooling. Infrastructure as a Service: The lowest layer is known as Infrastructure as a Ser-vice (IaaS). CSP developers, a highly scaled and elastic computing infrastructure that is used to run applications. This infrastructure can be comprised of virtualized servers, storage, databases, and other items. Two well-known examples are the Amazon Elastic Compute Cloud, a commercial platform as part of Amazon.com's Web Service platform, and Eucalyptus, an open-source platform that the same functionality.

4.3.1 Entities Involved:

Cloud actors/entities can be divided into two main categories: A) CSP or Service Provider those who provide a service; and B) Cloud Service User (Users) those who use a service. Within Cloud Computing the between the role played by a service provider and a user can be blurred. The service provider could also be the user of another service e.g. when infrastructure is the service. The exact de notion of whether an entity is a provider or user is dependent on the context of the interaction and the service being. Some service providers will do services at all three service levels, just one particular level of service and have their own internal IaaS infrastructure.

A possibility could be that CSP providers are either: a) Infrastructure Service Providers those that IaaS and own and run the data centres that physically house the servers and software; or b) Service Providers those that PaaS or SaaS services. And that Cloud Service Users are either: A) Platform Users are users who buy into a service provider's platform e.g. Facebook; and B) Consumers are service users who use either SaaS or IaaS services.

Defining the Cloud:

The term `cloud' has been used traditionally as a metaphor for networks and helps abstract over their inherent complexity. This term, however, has evolved to encompass the transparency between the technological infrastructure of the CSP and the consumer’s point of view. A cloud can be one of the following types:

Public Constituting publicly accessible services that are accessed over the Internet and are often described using the term \The Cloud".

Private These are private services deployed on private networks. Such clouds may also be managed by third parties.

Hybrid A combination of services both privately and publicly. For example, core-services may be on a private cloud; other services originate from public clouds.

4.4 Benefits of Cloud Computing:

Many of the benefits to be had when using Cloud Computing are the lower costs associated. At the infrastructure level, virtual images can be scaled and contracted with complete disregard for any associated hardware costs such as equipment procurement, storage, maintenance, and use. This is all taken care of by the service provider and will be factored into the payment for the service: capital expenditure has been converted into operational expenditure. Resources within the cloud can be treated as a commodity, an `unlimited' medium. At both the platform and software level, similar benefits are seen. Aspects such as software installation, deployment, and maintenance are virtually non-existent. This is taken care of by the provider within their infrastructure. The service user only pays technical support.

Service providers at the SaaS level, often tout features that allow users to collaborate and interact with each other, in real-time, within the scope of the service being needed. For example, Google Docs allows users to edit documents simultaneously and for users to see each other's edits in real-time. Moreover, the provision of platform and software `as a service' allows cloud service users the ability to aggregate services together either for their use or to promote as another service i.e. Mashups. The aggregation could imply the combination of functionality from several services or the change/combination of output from the services involved.

Remark. Service aggregation is a good example of outlining how a service user can become a service provider.

4.4.1 Cloud Security Issues:

Security issues come under many guises both technical and socio-technical in origin. To cover all the security issues possible within the cloud, and in-depth, would be herculean|a task not suited even for Heracles himself. The Cloud Security Alliance identifies seven threats to cloud computing that can be interpreted as a classification of security issues found within the cloud. They are:

1. Abuse and Nefarious Use of Cloud Computing

2. Insecure Application Programming Interfaces

3. Malicious Insiders

4. Shared Technology Vulnerabilities

5. Data Loss/Leakage

6. Account, Service

7. Unknown Risk Pro

Similarly, describing PBE's use as part of a crypto-system was also a necessary evil, it established not only how PBE schemes could be deployed (see Section 9.8) but also points of contention within such deployment. Of which the most notable issues were those surrounding key management such as constructing, issuing, and revocation. Furthermore, the use of PBE identified three different modes of operation that describe the three different ways in which PBE schemes can be leveraged within a crypto-system |see Section 9.8. When combined with the cloud setting, two different sets of scenarios emerged based upon whether the service user's or CSP's data was to be protected.

PBE schemes can be used to protect service user's data in three different scenarios: Scenario I saw the inclusion of PBE within a service; Scenario II saw the provision of PBE as-a-Service, and Scenario V saw PBE being deployed by the user. In each of these three scenarios, PBE can be used by service users to specify precisely with whom they wish to share their data, for what purpose, and for how long. Although Scenario V may be a privacy zealot's ideal choice| they are in full control|its practical feasibility has yet to be determined; the ability for service users' to act competently as a Key Authority is still unclear. The remaining two scenarios, on the other hand, do appear to be more promising. However, these scenarios in themselves do present a dilemma between usability and the guarantees made over end-to-end security.

When looking to protect CSP's data, PBE can facilitate keyword searches with complex queries over encrypted data: Scenario III by the CSP; and in Scenario IV by a service user. This use of PBE is rather interesting in that the focus of these scenarios is on the CSP and not service user, and is most certainly worthy of further investigation.

The use of PBE within the cloud appears to be concentrated at both the PaaS and SaaS service layers. Though some may be surprised at PBE's lack of use at the IaaS layer, this was not unexpected. The primary interaction between a service user and CSP at this level is over managing virtual machines: Not much else happens.

4.5 Main Concept:

4.5.1 A Survey on Protection of Multimedia Content in Cloud Computing

In this Modern Online World Security Plays an Important role. Cloud Computing algorithms have the Capability to Disable Privacy. Multi-Media is the Clear Integration of data, text, image, audio, video in one application. In this Paper We Introduced Algorithm with Good Concept to Protect 2-D Videos, 3-D Videos, Audio, and Image. This new type of Cloud Computing system detects Duplicate and Copyrighted material in the Online.

Cloud computing is a Practical approach for Making convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort and also service provider interaction. Cloud computing provides a Computing paradigm where computing resources make available as service of the Internet. This paradigm provides facility to Customers to Consumers and businesses without installation of this application and provides access to personal files at any computer with internet access. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. In this Cloud Services, Large Pool of Systems Can be able to be connected. With the advance of Cloud Computing technology the cost of computation, application hosting, content storage, and delivery is reduced significantly/ Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. This also provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications. Upon these benefits, there are privacy and security concerns too. For the past few years, cloud-based storage has oscillated somewhere between a replacement strategy for existing back-up storage solutions (i.e. tape) and a typically inexpensive but complex real-time storage solution for online web properties and enterprises. Data transmission and storage can fall under many regional regulations involving the security and availability of personal information.

Cloud Providers offer services that can be grouped into three categories. 1. Software as a Service (SaaS): In this model, a complete application is offered to the customer, as a service on demand. A single instance of the service runs on the cloud & multiple end users are serviced. On the customer's side, there is no need for upfront investment in servers or software licenses, while for the provider, the costs are lowered, since only a single application needs to be hosted & maintained. Today SaaS is offered by companies such as Google, Salesforce, Microsoft, Zoho, etc. 2. Platform as a Service (PaaS): Here, a layer of software or development environment is encapsulated & offered as a service, upon which other higher levels of service can be built. The customer has the freedom to build his applications, which run on the provider's infrastructure. To meet the manageability and scalability requirements of the applications, PaaS providers offer a predefined combination of OS and application servers, such as the LAMP platform (Linux, Apache, MySQL, and PHP), restricted J2EE, Ruby, etc. Google App Engine, Force.com, etc are some of the popular PaaS examples. 3. Infrastructure as a Service (IaaS): IaaS provides basic storage and computing capabilities as standardized services over the network. Servers, storage systems, networking equipment, data centre space, etc. are pooled and made available to handle workloads. The customer would typically deploy his software on the infrastructure. Some common examples are Amazon, Go Grid, Tera, etc.

Understanding Public and Private Clouds Enterprises can choose to deploy applications on Public, Private or Hybrid clouds. Cloud Integrators can play a vital part in determining the right cloud path for each organization. Public Cloud Public clouds are owned and operated by third parties; they deliver superior economies of scale to customers, as the infrastructure costs are spread among a mix of users, giving each client an attractive low-cost, ―Pay-as-you-go‖ model. All customers share the same infrastructure pool with limited configuration, security protections, and availability variances. These are managed and supported by the cloud provider. One of the advantages of a public cloud is that it may be larger than an enterprise cloud, thus providing the ability to scale seamlessly, on-demand. Private Cloud Private Clouds are built exclusively for a single enterprise. They aim to address concerns on data security and offer greater control, which is typically lacking in a public cloud. There are two variations to a private cloud: - On-premise Private Cloud: On-premise private clouds, also known as internal clouds are hosted within one's own data center. This model provides a more standardized process and protection but is limited in aspects of size and scalability. IT departments would also need to incur the capital and operational costs for the physical resources. This is best suited for applications that require complete control and configurable to the infrastructure and security. - Externally hosted Private Cloud: This type of private cloud is hosted externally with a cloud provider, where the provider facilitates an exclusive cloud environment with a full guarantee of privacy. This is best suited for enterprises that don't prefer a public cloud due to the sharing of physical resources. Hybrid Cloud Hybrid Clouds combine both public and private cloud models. With a Hybrid Cloud, service providers can utilize third party Cloud Providers fully or partially thus increasing the flexibility of computing. The Hybrid cloud environment is capable of providing an on-demand, externally provisioned scale. The ability to augment a private cloud with the resources of a public cloud can be used to manage any unexpected surges in workload.

Cloud Computing Benefits Enterprises would need to align their applications, to exploit the architecture models that Cloud Computing offers. Some of the typical benefits are listed below: 1. Reduced Cost There are several reasons to attribute Cloud technology with lower costs. The billing model is paying as per usage; the infrastructure is not purchased thus lowering maintenance. The initial expense and recurring expenses are much lower than traditional computing. 2. Increased Storage With the massive Infrastructure that is offered by Cloud providers today, storage & maintenance of large volumes of data is a reality. Sudden workload spikes are also managed effectively & efficiently since the cloud can scale dynamically. 3. Flexibility This is an extremely important characteristic. With enterprises having to adapt, even more rapidly, to changing business conditions, speed to deliver is critical. Cloud computing stresses on getting applications to market very quickly, by using the most appropriate building blocks necessary for deployment.

1. Cloud Computing Challenges Despite its growing influence, concerns regarding cloud computing remain. In our opinion, the benefits outweigh the drawbacks and the model is worth exploring. Some common challenges are 1. Data Protection Data Security is a crucial element that warrants scrutiny. Enterprises are reluctant to buy an assurance of business data security from vendors. They fear losing data to competition and the data confidentiality of consumers. In many instances, the actual storage location is not disclosed, adding to the security concerns of enterprises. In the existing models, firewalls across data centres (owned by enterprises) protect this sensitive information. In the cloud model, Service providers are responsible for maintaining data security and enterprises would have to rely on them.

2. Data Recovery and Availability All business applications have Service level agreements that are stringently followed. Operational teams play a key role in the management of service level agreements and runtime governance of applications. In production environments, operational teams support appropriate clustering and Failover Data Replication System monitoring (Transactions monitoring, logs monitoring, and others) Maintenance (Runtime Governance) Disaster recovery Capacity and performance management If, any of the above-mentioned services are under-served by a cloud provider, the damage & impact could be severe.

3. Management Capabilities Despite there being multiple cloud providers, the management of platform and infrastructure is still in its infancy. Features like „Auto-scaling for example, is a crucial requirement for many enterprises. There is huge potential to improve on the scalability and load balancing features provided today.

4. Regulatory and Compliance Restrictions. In some of the European countries, Government regulations do not allow customer's personal information and other sensitive information to be physically located outside the state or country. To meet such requirements, cloud providers need to set up a data centre or a storage site exclusively within the count to try to comply with regulations. Having such an infrastructure may not always be feasible and is a big challenge for cloud providers.

With cloud computing, the action moves to the interface — that is, to the interface between service suppliers and multiple groups of service consumers. Cloud services will demand expertise in distributed services, procurement, risk assessment, and service negotiation — areas that many enterprises are only modestly equipped to handle.

4.5.2 Main Concept in this Research:

In this Research We Analysed the new type of approach for Protecting the Multi-Media Content in the Cloud.

EXISTING SYSTEM:

- The problem of protecting various types of multimedia content has attracted significant attention from academia and industry. One approach to this problem is using watermarking, in which some distinctive information is embedded in the content itself and a method is used to search for this information to verify the authenticity of the content.

- Many previous works proposed different methods for creating and matching signatures. These methods can be classified into four categories: spatial, temporal, color, and transform-domain. Spatial signatures (particularly the block-based) are the most widely used.

- YouTube Content ID, Vobile VDNA, and Mark Monitor are some of the industrial examples which use fingerprinting for media protection, while methods such as can be referred to as the academic state-of-the-art.

4.5.3 DISADVANTAGES OF EXISTING SYSTEM:

- The Watermarking approach may not be suitable for already-released content without watermarks in them. Watermarking may not be effective for the rapidly increasing online videos, especially those uploaded to sites such as YouTube and played back by any video player.

- The spatial signature's weakness is the lack of resilience against large geometric transformations. Temporal and color signatures are less robust and can be used to enhance spatial signatures. Transform-domain signatures are computationally intensive and not widely used in practice.

4.5.4 PROPOSED SYSTEM:

The mobile Cloud computing has many servers and each server maintains a small cache storage system. When the task is received by the server, the server searches in its cache whether the cache has related task id, if the server has the task the task is performed from the cache and task is completed on the server. If the server does not have the id, then the task id is broadcasted to the nearby servers. And the servers search in its own cache storage system. If any one of the cache has the relates task then the server gives positive acknowledgement to the server which has the task. Then the server shares the task to the server which gave the positive acknowledgement. Hence the task is computed and returned the result. Thereby we reduce the energy of computation and task offloading. All the new task are not stored in the cache memory and so cache space is also used efficiently.

- Appropriate use of these security standards can benefit the application greatly, improving security and response times and reducing server load
- Implemented with servers which can optionally have a local server with in-line cache. This optional server cache independent data grid on each server, which maintain serving cache for server-side cache. This is called near server-side cache. A server-side cache is fast because it supports in line memory content for entire cached data which is stored remotely
- Applied optimization method to save time and energy, bandwidth consumption etc. even searching on nearby servers takes less time and consume less energy as compare to sending task directly on main cloud datacenter.

4.5.5 ADVANTAGES OF PROPOSED SYSTEM:

- Accuracy.
- Computational Efficiency.
- Scalability and Reliability.
- Cost Efficiency.
- The system can run on private clouds, public clouds, or any combination of public-private clouds.

- Our design achieves rapid deployment of content protection systems because it is based on cloud infrastructures that can quickly provide computing hardware and software resources.
- The design is cost-effective because it uses the computing resources on demand.
- The design can be scaled up and down to support varying amounts of multimedia content being protected.

4.5.6 The architecture of multimedia content Protection of the Proposed System

The original antenna is chosen to be a square to excite two modes with close resonant frequencies required for circular polarization. Asymmetry in the structure is introduced through edges so that the coaxial line feed point is along the diagonal of the patch. Both LHCP and RHCP can be obtained by shifting the feed point to accurate positions on the diagonal axis.

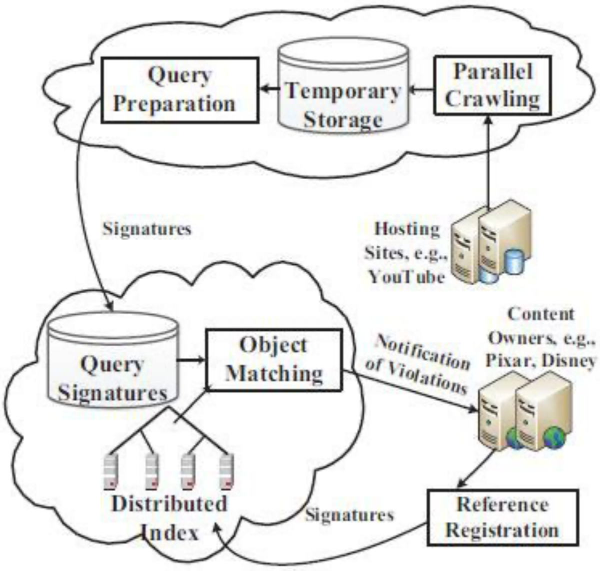


Figure 4:1 The architecture of multimedia content Protection of the Proposed System

Multimedia typically refers to the combination of audio, video, images. To protect these multimedia contents from being pirated here is a new design for large-scale multimedia content protection systems. This design leverages cloud infrastructure to improve cost efficiency, scalability, and elasticity. The proposed system can protect 2D videos, 3D videos, images, audio clips. The system comprising the steps (a) method to create the signature (b) distributed matching engine for multimedia objects. Extracting features from the multimedia content to form signature data. The signature data comprising a combination of at least two of a visual signature, an audio signature, a depth signature, or metadata, also identify online content to be processed for copy detection and finally comparing the signature data against the online content data signatures, and determining whether this online content is a copy of the multimedia content.

The proposed system has multiple components as shown in the figure. The cloud providers are more efficient and/or provide more cost-saving for different computing and communication tasks. For example, a cloud provider offering lower cost for inbound bandwidth and storage can be used for downloading and temporarily storing videos from online sites, while another cloud provider (or private cloud) offering better compute nodes at lower costs can be used to maintain the distributed index and to perform the copy detection process. The proposed system can be deployed and managed by any of the three parties mentioned in the previous section: content owners, hosting sites, or service providers.

4.5.7 Distributed Index: Maintains signatures of objects that need to be protected;

- Reference Registration: Creates signatures from objects that content owners are interested in protecting, and inserts them in the distributed index;
- Query Preparation: Creates signatures from objects downloaded from online sites, which are called query signatures. It then uploads these signatures to common storage;
- Object Matching: Compares query signatures versus reference signatures in the distributed index to find potential copies. It also sends notifications to content owners if copies are found;
- Parallel Crawling: Downloads multimedia objects from various online hosting sites.

The Distributed Index and Object Matching components form what we call the Matching Engine. The second and third components deal with signature creation. For the Crawling component, we designed and implemented a parallel crawler and used it to download videos from YouTube. The details of the crawler are omitted due to space limitations.

The proposed system mainly uses Signature Creation which is designed to handle different types of multimedia objects. The system abstracts the details of different media objects into multidimensional signatures. The signature creation and comparison component are media-specific, while other parts of the system do not depend on the media type. Our proposed design supports creating composite signatures that consist of one or more of the following elements:

- Visual signature: Created based on the visual arts in multimedia objects and how they change with time.
- Audio signature: Created based on the audio signals in multimedia objects;
- Depth signature: If multimedia objects are 3-D videos, signatures from their depth signals are created
- Metadata: Created from information associated with multimedia objects such as their names, tags, descriptions, format types, and IP addresses of their uploaders or downloaders.

4.6 CONTENT FILTERING AND CLOUD-BASED INTRUSION DETECTION SYSTEM

The prime objective of this proposal is to provide a secure platform for the organizations/ institutions which are involving directly or indirectly with confidential information and having the resources of high usage. This project will complain about the needs of the professional institutions in the society offering e-learning activities like content generation, distribution, training, preparation relating to e-content, and its maintenance in both academia and research areas. When it comes to sharing the user's ideas with experts and software tool providers over the internet, security has become the prime concern. The intruders/hackers maybe after high-speed connections can send malicious viruses and worms to blackening the reputation. To ensure security to the resources like software tools, hardware equipment, operating system, and e-content the institution has taken necessary precautions. In this context, to overcome the threats, the installation of firewalls both hardware and software in nature are of high importance. Though the measures exist, the hackers/intruders are coming up with the latest techniques to hijack the networking system. As the users are increasing and mostly depending on the internet to extract and use the required information / open-source software tools available, to carry out their research and academic projects from the global arena. It is necessary to inspect the incoming and outgoing information, which may cause damage or loss of digital information, resources, and tools. In this context, I propose an intruder detection system against vulnerabilities over the internet where the information would be filtered by using a solid hardware firewall with proper configuration and installation of software. This will help the institution to stop intruders from accessing our system. Providers can keep the internet link to the outside world, but it can't share the resources unless the user has granted the privilege. With a firewall in place, the users will still have typical email access, but chat and other interactive programs will require the users to take an extra step to grant access before use.

4.6.1 OBJECTIVE - SIGNIFICANCE:

The proposal entitled "Content Filtering: An Intrusion Detection System" aims at achieving the following goals/objectives, but not limited to

a. A Secure Cross-Platform networking model.
b. Detection and Prevention of Intrusions from the internet.
c. User i.e., Student, Staff, and Research Scholar can have access to the required content / open-source tool, preventing unwanted ones.
d. Managing Services and Tools efficiently.
e. Identification of worms, viruses, masquerading, Phishing, etc.,
f. Prevention of data centres from attacks.

The project proposal will be closely associating with department / institutional needs. The institution shall have to maintain the computers, software, and other tools to cater to the needs of the students, faculty, and researchers. To provide better qualitative knowledge, the institution is facilitating with high-end systems, internet connectivity with high speed. To carry out their academic and research activities, everyone is directly or indirectly dependent on the internet. In this context, the users of the institution shall have to aware of the viruses, worms, and threats which causes to crash of the tools like hardware, software, data centers, and other resources. Sometimes the entire network system may be crashed. This needs of security like the police to watch/inspect the information coming in and going out of the institution. Hence, there must be a watch on the flow of information which may be represented by pictures, text, audio, and video formats. Hence, I strongly believe the proposed project is relevant and fulfills the needs of the department and institution in society. Please refer Annexure I for the proposed system

4.6.2 NATIONAL & INTERNATIONAL SCENARIO: PROPOSED SYSTEM

Enterprise businesses are being transformed to meet the evolving challenges of today's global business economy. Innovations and new business models are enabling new kinds of productivity, competitive advantage, revenue growth, and efficiency that drive the top line and the bottom line. Security is fundamental to the ability to leverage, with confidence, these rich services that are critical to business success. The comprehensive and diverse security portfolio enables the complex security challenges faced in this environment to be addressed through an integrated, defense-in-depth approach to security that is embedded in end-to-end solution architectures. In the proposed system, the Network Security Integration solution describes how to extend this integrated, defense-in-depth approach to security to encompass the mobility services offered by a LAN. Mobility is a critical service for enterprises, offering employees greater flexibility, and enabling increased productivity, through pervasive access to network resources and applications. However, this service offering must comply with the defined network security policies and integrate with the end-to-end network security strategies to be compliant, effective, and efficient. Network Security is an ongoing process of defining security policies, implementing proactive security measures to enforce them, monitoring the network to obtain visibility into activity, identifying and correlating anomalies, mitigating threats and reviewing what occurred to modify and improve the security posture.

Figure 4:2 National & International Scenario: Proposed System

A wired or wireless network is only one of the attack vectors against a network. While a WLAN network must be secure and able to protect itself from attack, a network-wide security solution that only addresses WLAN-related attacks is dangerously unbalanced. Mobile network clients need to be protected on all interfaces at all locations, enterprise networks need to be protected on all their perimeters, and monitoring and anomaly detection are required regardless of the source of network traffic. Ideally, the same sets of tools and interfaces should be used to provide these baseline security functions as it reduces operational costs, reduces the risk of misconfiguration, and avoids the creation of an unbalanced security architecture that can be simply bypassed.

4.6.3 Security Solution Components

The Secure Wireless Architecture is built on the core architectures for the branch and campus networks. The Secure Network Architecture describes the integration and collaboration of security solutions with the Unified Networks to provide a common security framework for networks regardless of the client access mechanism. The core components of the Secure Architecture include Unified Network, Intrusion prevention, Rogue detection and mitigation, Access control, Traffic encryption, User authentication, RF interference, and DoS monitoring, Security vulnerability monitoring and auditing, Infrastructure hardening—MFP, infrastructure device authentication, CSA, NAC appliance, Firewalls, IPS, MARS.

4.6.4 Solution Architecture

The purpose of the Secure Network Solution Architecture is to provide common security services across the network for wireless and wired users and enable collaboration between wireless and network security infrastructure for layered security architecture. This architecture is equally applicable in both campus and department deployments. The core components of this architecture are:

- Unified Network Architecture
- Campus Architecture
- Department Architecture

The Unified Network Architecture provides the core mobility services platform securing the wireless environment as well as all the functions required to secure the wireless deployment itself. The underlying campus and department architectures provide a secure high performance, high availability network platform for mobility services. This provides a common wired and wireless platform for the integration of security services, allowing common security architecture to be developed for all network clients and traffic types.

4.6.5 Unified Network System

WLANs in the enterprise has emerged as one of the most effective means of connecting to a network. The Network is a unified wired and wireless network solution that addresses the wireless network security, deployment, management, and control aspects of deploying a wireless network. It combines the best elements of wireless and wired networking to deliver secure, scalable networks with a low total cost of ownership. Client devices, Access points, Controllers, network management, and mobility services work together to deliver a unified enterprise-class solution.

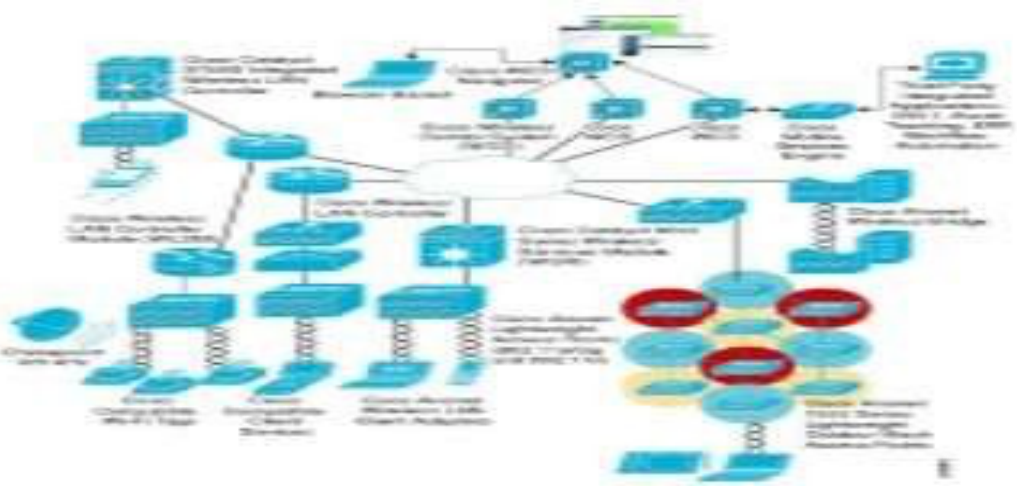


Figure 4:3 Unified Network System

The components required for secure deployment and operations of a wireless network are built into the Cisco Unified Network infrastructure. Leveraging Wireless LAN controllers, access points and wireless management systems provide comprehensive wireless security, reducing capital costs while streamlining security operations. Leveraging the features and functions of our proposed network security portfolio delivers a greater degree of control over wired and wireless networks, users, and their traffic. Further, supplementing wireless security with wired network security provides layered defenses that deliver more thorough protection, with greater accuracy and operational efficiency for both network operations and security operations teams within the departments. Wireless, due it's over the air transmission, has unique security requirements. The primary security concerns for a network are:

- Rogue access points and clients that can create backdoor access to the network.
- Hacker access points, such as evil twins and honey pots
- Denial of service that disrupts the network.
- Network reconnaissance, eavesdropping, and traffic cracking.
- Controlling the network's users connect to, especially when they are outside of the organization.
- Security for guest users.

Security event management and reporting on all of these functions, complete with physical location tracking of where the security event took place on the network, is key to any robust security solution. All of these concerns are addressed by security technologies built-in in the controllers, access points, and CS management system. The same gear that provides connectivity to users also provides security for the entire deployment. A built-in intrusion prevention system detects and mitigates rogue access points and clients, as well as DoS attacks, hacker access points, network reconnaissance, eavesdropping, and attempted authentication and encryption cracking. Further, it can provide wireless IPS monitoring from the same access points that service user traffic, as well as provide full- time dedicated wireless IPS monitoring. Providing both approaches enables site-specific flexibility based on network security policies, which reduces the high infrastructure costs associated with stand-alone wireless intrusion prevention systems. Networks should be self-defending. Providing a hardened network core that is impenetrable to attacks is better than simply detecting an attack after the damage is done. Secure guest access management is also addressed in the Unified Network infrastructure, providing captive guest user portal, network segmentation, and full guest management functionality. Finally, wrapping all this together is the Security management system.

4.6.6 Secure Wireless Architecture

The Secure Wireless Solution Architecture consists of a WLAN security component and network security components. The Cisco Unified Wireless Network provides the WLAN security core that integrates with other Cisco network security components to provide a complete solution. The Cisco Unified Wireless Network Architecture provides a mechanism to tunnel client traffic to the wireless LAN controller in a campus service block. The services block provides a centralized location for applying network security services and policies such as NAC, IPS, or firewall. In addition to the components protecting the network in the services block, the Cisco Security Agent provides an additional protection network, as well as protecting the mobile client. Wired/wireless collaboration does not just mean putting more boxes in the network. It is the purpose-built linkages that have been built between Cisco's wired and wireless security technologies to deliver a superset of security functionality and protection.

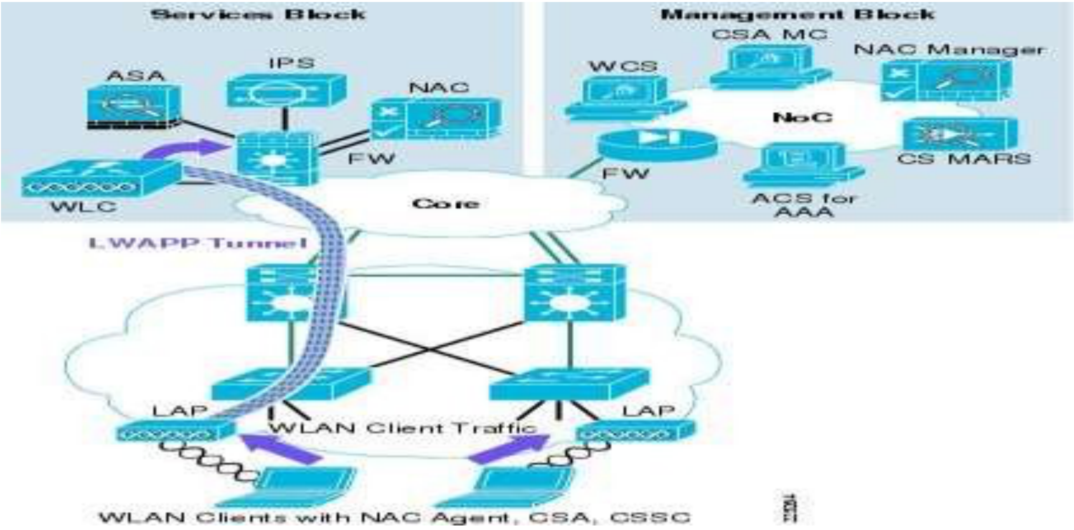


Figure 4:4 Secure Wireless Architecture

4.6.7 Campus Architecture

The overall campus architecture is more than the fundamental hierarchical router and switch design. While hierarchies such as access, distribution, and core are fundamental to how to design and build campus networks, they do not address the underlying questions about what a campus network does. The campus network provides services that are used to build secure wireless solutions. Services such as these provide the foundations for the Secure Solution are High availability, Access services, Application optimization, and protection services, Virtualization services, Security services, and operational and management services.

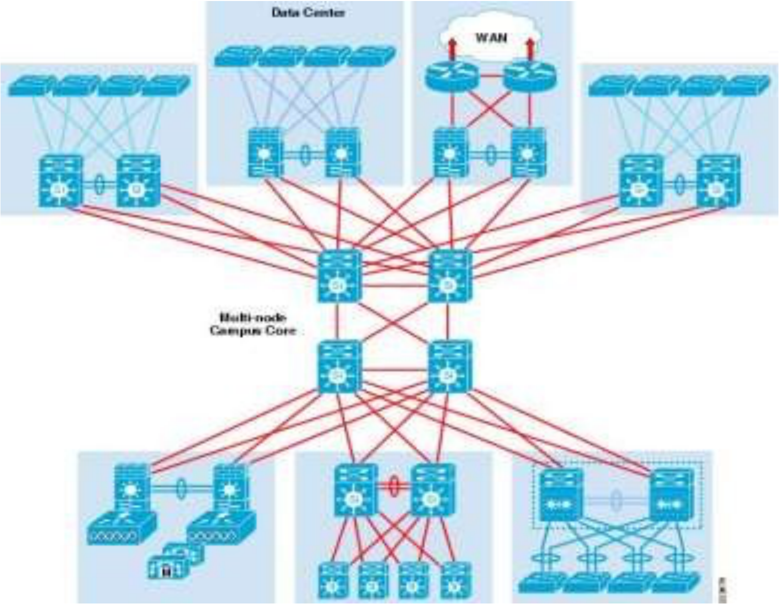


Figure 4:5 Campus Architecture

4.6.8 Department Architecture

The full-service branch provides the same solutions and services to a branch as are available for the campus. This includes security and wireless, and the Secure Wireless solution is equally applicable for department deployments as it is for the campus. There are many LAN/WLAN, firewall, and NAC options for a department, including an H-REAP, WLAN Controller Module (WLCM), 21XX WLC, or larger WLCs, PIX, ASA, or IOS Firewalls, NAC appliances, and IPS appliances.

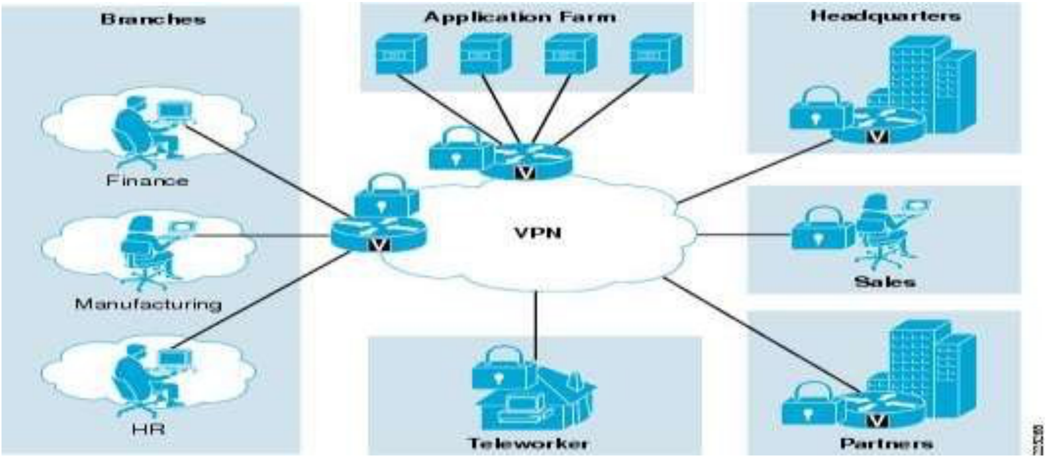


Figure 4:6 Department Architecture

Due to the increased mobile traffic, mostly multimedia demand which includes Audio, video, and gaming are produced by smartphones or other end devices that can produce a lot of congestion on the core network. Typical IP protocols won't work efficiently in terms of QoE, delay, and throughput. Mobile Cloud Computing ICN can provide these services in an efficient mannerist support's naming scheme in which the user is transparent to the underlying processes (e.g. location of processes/server), the user is concerned with high-level names [3]. In [13], they used a cluster caching approach in Mobile Cloud Computing ICN which reduced the packet loss ratio and increased the transfer time ratio.

A smart caching mechanism in[8] used an edge environment over a Mobile Cloud Computing ICN architecture in which they used 1) Location prediction 2) Smart cache using machine learning method for the placement of mobile multimedia content on the edge nodes and at the end, a smart cache replacement algorithm and there result showed that there proposed algorithms performed well against the comparative techniques which include increased hit ratio and reduced access time.

A popularity prediction caching is proposed by leveraging Mobile Cloud Computing ICN architecture; they designed a chunk level cache eviction policy that predicts video chunk's future popularity. In this strategy, they analyzed early behavior and user request behavior relationship between the same video files neighboring chunks by doing this they monitored the user viewpoint behavioral aspect and chunks relationship. If the predicted chunk popularity has the highest count that chunk will be placed and whose predicted count is outdated will be evicted from the cache and there model increased the efficiency over LFU and LRU [14].

Three types of Adaptive Bit Rate (ABR) algorithms rate based, buffer based and hybrid-based for adaptive video streaming have been tested in [15] under the influence of QoE in a Mobile Cloud Computing ICN environment. Based on their evaluation they confirmed that re-buffering happens in throughput-based approaches due to the factor of hit ratio. Rate based algorithm bitrate decreased due to the count of throughput but QoE is better than hybrid based vice versa but buffer based QoE and bitrate is low because of its strict policies and no buffering state. There work concluded that ABR performance depends upon user preferences, but tested algorithms don't work on different situations.

Caching the videos at the edges of the networks can reduce congestion at the backhaul. The author in [16] introduced a proactive caching technique by leveraging 5G- Mobile Cloud Computing ICN approach. In their smart caching technique, they used non-negative matrix factorization for the prediction of the future rating of consumer preferences of videos but the shortcoming of this technique its inaccurate for unpopular videos. So, they also used historical prediction into consideration to cope with this problem there works increased the hit ratio and the retrieval video delay but under the mobility, their techniques don't perform well.

K.Hasan et al[17] proposed a lightweight collaborative cache scheme by leveraging Mobile Cloud Computing ICN perspective in which cache placement is dependent on the routers position and the popular videos have to be cached at the routers which are closer to the user and this scheme adaption isn't dependent on the prior knowledge about popular videos but its adapts according to the user request. Video placement on the cache of the router is dependent on the router threshold because different routers can have different threshold due to their different topologies. Results showed that their scheme reduced no hop count and publisher load, but the drawback of their approach is a large amount of redundancy across the network.

References:

1) Investigation on the Data Protection in the Cloud using Predicate Based Encryption International Journal of Computer Science and Information Technology Research UGC approved with ISSN 2348-120X (Online) Vol. 6, Issue 4, pp: (61-65), Month: October - December 2018.http://www.researchpublish.com/journal/IJCSITR/Issue-4-October-2018-December-2018/0

2) Cloud Security Risk Factors and Security Issues in current trends research paper by Dr.K.Sai Manoj accepted and Presented in Scopus Based 2nd International Conference on Materials, Applied Physics, and Engineering (ICMAE 2018) at Indore. Proceedings of the 2018 First international conference on Materials, Applied Physics, and Engineering. After Clear scientific check, this Paper was already Promoted to Science Publication Corporation.

3) Literature survey on the destruction of attaches with MH HOP to HOP to HOP-AODV Routing Protocol in Vehicular Ad-hoc Network, Dr.K.Sai Manoj, Mrudula Kudaravalli, © December 2017 | IJIRT | Volume 4 Issue 7 | ISSN: 2349-6002

4) Mmmmmm I. Hedenfalk, D. Duggan, Y. Chen, M. Radmacher, M. Bittner, R. Simon, P. Meltzer, B. Gusterson, M. Esteller, O. P. Kallioniemi, B. Wilfond, A. Borg, and J. Trent, "Gene Expression profiles in hereditary breast cancer," N Engl J Med, vol. 344, no. 8, February 2001, pp. :539–548.

5) M. M. Hossain, M. R. Hassan, and J. Bailey, "ROC-tree: A Novel Decision Tree Induction Algorithm Based on Receiver Operating Characteristics to

Classify Gene Expression Data," Proc. SIAM International Conference on Data Mining, Atlanta, Georgia, USA, April 2008, pp. 455–465.

6) S. Pandey, W. Voorsluys, M. Rahman, R. Buyya, J. Dobson, and K. Chiu, "A Grid Workflow Environment for Brain Imaging Analysis on Distributed Systems," Concurrency and Computation: Practice and Experience, Jul. 2009, DOI:10.1002/cpe.1461.

7) J. Yu and R. Buyya, "Gridbus workflow enactment engine," in Grid Computing: Infrastructure, Service, and Applications, L. Wang, W. Jie, and J. Chen Eds, CRC Press, Boca Raton, FL, USA, April 2009, pp. 119–146.

8) Survey on Protection of Multimedia Content in Cloud Computing, Dr. K.Sai Manoj, Mrudula Kudaravalli, International Journal of Computer Science and Mobile Computing - Vol.6 Issue.11, November- 2017, pg. 7-11 http://ijcsmc.com/docs/papers/November2017/V6I11201705.pdf

9) F. Cappello and H. Bal, "Toward an international computer science Grid," Proc. 7th IEEE International Symposium on Cluster Computing and the Grid (CCGRID'07), pp 3–12, Rio, Brazil, 2007. IEEE.

10) X. Chu, K. Nadiminti, C. Jin, S. Venugopal, R. Buyya, "Aneka: Next-Generation Enterprise Grid Platform for e-Science and eBusiness Applications," Proc. 3rd IEEE International Conference on e-Science and Grid Computing, Bangalore, India, December 2007.

11) K. Phani Srinivas "Clock Harmonization during Time-Variant Underwater International Journal of Engineering Trends and Technology (IJETT). V4(4):1158-1163 Apr 2013. ISSN:2231-5381. www.ijettjournal.org. published by a seventh sense research group.

12) Manas Pulipat, K. Phani Srinivas, ―Comparison of Various Short Range Wireless Communication Technologies withNFC‖, International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064, Volume 2 Issue April 2013.

13) J. F. Yang and Z. B. Chen, ―Cloud Computing Research and Security Issues,‖ 2010 IEEE International Conference onComputational Intelligence and Software Engineering (CSE), Wuhan pp. 1-3, DOI= 10-12 Dec. 2010.

14) S. Zhang, S. F. Zhang, X. B. Chen, and X. Z. Huo, ―Cloud Computing Research and Development Trend,‖ In Proceedings of the 2010 Second International Conference on Future Networks (ICFN '10). IEEE Computer Society, Washington, DC, USA, pp. 93-97. DOI=10.1109/ICFN.2010. 58.

15) J. J. Peng, X. J. Zhang, Z. Lei, B. F. Zhang, W. Zhang, and Q. Li, ―Comparison of Several Cloud Computing Platforms,‖ 2009 Second International Symposium on Information Science and Engineering (ISISE '09). IEEE Computer Society, Washington, DC, USA, pp. 23-27, DOI=10.1109/ISISE.2009.94.

16) S. Zhang, S. F. Zhang, X. B. Chen, and X. Z. Huo, ―The Comparison between Cloud Computing and Grid Computing,‖ 2010 International Conference on Computer Application and System Modeling (ICCASM), pp. V11-72 - V11-75, DOI= 22-24 Oct. 2010.

17) A comprehensive review of wireless body area network Khalid lHasan Journal of Network and Computer Applications Volume 143, 1 October 2019, Pages 178-198

18) M. M. Alabbadi, ―Cloud Computing for Education and Learning: Education and Learning as a Service (ELaaS),‖ 2011 14th International Conference on Interactive Collaborative Learning (ICL), pp. 589 – 594, DOI=21-23 Sept. 2011.

19) P. Kalagiakos ―Cloud Computing Learning,‖ 2011 5th International Conference on Application of Information and Communication Technologies (AICT), Baku pp. 1 - 4, DOI=12-14 Oct. 2011.

20) Content Filtering and cloud-based intrusion detection system, Dr.K.Sai Manoj, Global Journal of Engineering Science and Research Management – January 2018

21) P. Mell and T. Grance, ―Draft NIST working definition of cloud computing - vol. 21, Aug 2009, 2009.

22) Sun Microsystems Unveils Open Cloud Platform,‖ [Online]. Available: http://www.sun.com/aboutsun/pr/2009-03/sunflash.20090318.2.xml,2 009.

23) W. Dawoud, I. Takouna, and C. Meinel, ―Infrastructure as a Service Security: Challenges and Solutions,‖ 2010 7th International Conference on Informatics and System, pp. 1-8, March 2010.

24) Andrew S. Tanenbaum, Computer Network [M]. 4th Edition, USA: Prentice-Hall, Sep 2003

25) Chen Bing, "Computer Engineering and Application" Research on Architecture of Network Security *[J]*, Vol38, No7, 2002.

26) Eric Maiwald, Network Security: a beginner's guide. USA: Osborne/McGraw-Hill, 2001.

27) Feng Dengguo, Computer Engineering g and Technology *[M].* 2th Edition, China: Science Press, 2010

28) Hu Daowen, Min Jinhua, Network Security *[M].* Bei Jing：Qing Hua Press 2004 [6]. Marcus Goncalves, Firewalls complete. USA: McGraw-Hill Companies, 1998

29) Wu Gongyi, Computer Network *[M].* Bei Jing: Qing Hua Press, 2009.

30) Zhang Shiyong, Network Security Principles and Applications *[M].* China:May 2003.

31) CISCO Firewall Technology user manual.

32) CISCO Wireless and Network Security Integration solution overview

Chapter 5

5 Chapter 5 : Experimental Search in Cloud Computing

5.1 Experimental Analysis

Grouped the mobile nodes in a MANETs under Mobile Cloud Computing ICN environment and investigated the impact of group mobility on the delay and throughput performance main concern of their research is to investigate content retrieval from the neighbouring nodes that are stored (cache) there based on the instinct of correlation between the nodes in the same group or between groups. They considered two arrangements cluster dense and cluster sparse and investigated both under fast mobility and slow mobility. Their results showed that under fast mobility throughput is degraded, and there is an improvement in the delay performance, and under slow mobility, the correlation among nodes had a negative impact on delay and throughput. Their cache allocation did not consider time and location, which means they used a static cache allocation technique.

An author in [21] adopted a Mobile Cloud Computing ICN approach content-centric network, In which groups were made when a specific mobile node request for content a group is created around its 10m range and the content that is requested if local storage available locally placement if not distribute the content into respected group members. They used Zipf distribution for content placement and for corporative group caching they used the "Hello" message mechanism to periodically

Check its local table, group table, and neighbouring nodes due to this mechanism, there is a communication overhead on the ad hoc network, but the Hit Ratio probability increased.

5.2 Important Concept

The phenomenon of Cloud Computing is promising, which ensures businesses increase efficiency alongside reducing their cost of production. Data protection and security in cloud computing are still crawling on its knees and need more research attention, although it has been deployed and used in the production environment.[21]

Data Security in Cloud Computing is an important area that should be given much attention. A large amount of data these days circulate in the cloud, which has given room for intruders and eavesdroppers to try and get hold of them. It is, therefore essential, for vigorous study on how to propose and implement a robust and functioning security mechanism that will prevent hackers from getting access to the data being transmitted to and fro in the cloud. Based on the information presented in this study, through the analysis of various papers and the insight gotten from the implementation of the proposed techniques, it is realized that majority of the papers give much attention to data confidentiality whilst few papers satisfy the three aspects of Security; Confidentiality, Integrity, and Availability.

5.3 Cyber Security in Cloud computing video streaming

Video streaming has become more popular over the past couple of years, and due to a huge amount of videos request put the load on the backhaul Mobile Cloud Computing ICN provides in-networking caching to cache videos near to user by considering user mobility to decrease load at backhaul. In our approach, we are considering group mobility under 5G- Mobile Cloud Computing ICN architecture to improve QoE. We placed the group mobility model (GMM) on the base station (BS) to capture mobile users' speed and direction and to predict whether a handoff will occur during video playback time. Users moving with similar speed and direction will form groups. A group with high mobility will have a link to the content router, and low mobility will get their videos from the base station. The preference model contains Zipf distribution to predict popular videos named content popularity model (CPM), and a kernel function is used for group members whose preference is different (DPM).

Then the cache decision model(CDM) will predict where to cache video at the base station or at the content router (CR).

The present Internet design was established upon a host-driven communication model. In that model, packets were used and exchanged between sender to receiver, and the path has to be created between them for communication which results in delay because data has to be accessed all the way from the provider and that was proper for adapting to the requirements of the early Internet users. Internet utilization has advanced nonetheless, with most users basically keen on accessing (Large set of) information independent of its physical localization [22]. A new paradigm Information-Centric Network is introduced to cope with the above mention problem.

Mobile Cloud Computing ICN provides flexibility in the network in terms of putting the content as near to the user as possible rather than a typical IP based retrieval process in which content is retrieved from the Content Provider, which degrades the QoE [23]. Mobile Cloud Computing ICN enables Named Data Network (NDN) and In-networking strategies, which supports mobility in 5G networks. NDN supports named based routing, In which accessing the content relies on the name of the data, it doesn't rely on the location/server [24]. In-networking enables caching of the content, which means routers and base stations in the 5G- Mobile Cloud Computing ICN architecture can store (cache) the content [25].

Mobility is one of the challenges in the wireless networks, and Mobile Cloud Computing ICN provides a better approach towards handling mobility. Typical IP networks use anchor-based strategies in which mobile node is connected to the content provider through an access point (AP) or base station (BS) when a handoff occurs only link changes, but data is fetched from a content provider who puts congestion on the backhaul. While Mobile Cloud Computing ICN provides Request and Reply content mechanism in which mobile nodes request the content, the nearest nodes check local storage if there forward the content [26]. Mobility in Mobile Cloud Computing ICN is the hottest research area; a lot of research is taken place, but most of them consider individual mobility. In [25], mobility patterns are identified through Janson density, but the consideration of pattern is only for the individual mobile node. Group mobility in Mobile Cloud Computing ICN can improve QoE and delay, while group mobility has been considered in Adhoc, WiMAX networks to increase the performance of routing protocols, shortened handover delays [27].

Video streaming became a crucial part of mobility when handoff will occur on how to maintain the quality of experience. According to figures of the cisco visual network index [28], mobile data traffic will increase by 46% in 2022 and in which 78% is video streaming. A lot of research has been done on mobile multimedia content, such as [29]. Most researchers focused on cache placement by taking count of individual mobility such as [25][30] but not group mobility.

5.4 Investigation on the Cloud Computing Security

5.4.1 Privacy Enhancing Technologies:

Privacy Enhancing Technologies (PET) enables clients to transact with providers securely, even if the clients do not trust the providers.PET denotes the set of tools and mechanisms that allow users to protect their privacy online against adversaries.

Blarkom et al. [2] define PET as a system of information and communication technology measures protecting informational privacy by eliminating or minimizing personal data, thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system. Privacy-preserving protocols [3], a class of PET, enable users to perform computation over cryptographically protected data.

Homomorphic encryption and searchable encryption schemes are notable privacy-preserving protocols. Homomorphic encryption is an asymmetric encryption technique, where algebraic operations are performed directly on the ciphertext, which represents the encryption of plain text. This was first introduced by Goldwasser et al. [4], where the authors performed a modular addition of two bits using multiplication of ciphertexts. Craig Gentry [5] designed a homomorphic encryption scheme that allows both addition and multiplication on the plain text through their ciphertexts.

Searchable encryption allows users to search for particular keywords on encrypted data. Public Key Encryption with Keyword Search (PEKS) [6] is one of the seminal works in the area of making encrypted data searchable.

The authors of PEKS propose to encrypt the message using the Public-Private key infrastructure. Along with this ciphertext, a Public-Key Encryption with Keyword Search (PEKS) of each keyword (the words that make up the message) is appended to the final message.

Although homomorphic encryption and searchable encryption are viable, proven ways of preserving the privacy of data in the cloud without compromising on the functionality, cryptography increases the computational and storage overhead on the server [7]. Computation over encrypted data, even though theoretically possible, is not yet practically feasible [8].

5.4.2 Need for trust: Remote Attestation

As the solutions proposed by PET are mostly in the theoretical realm, clients are forced to trust the cloud provider with the data and hope that the provider will not breach that trust. Trust is defined as "a particular level of subjective assessment of whether a trustee (cloud provider).

The client establishes trust in emotional and cognitive (evidence-based) grounds. Improvisation of the security on the server, the trust relationship between the client and server should be formed more based on cognitive, evidence-based grounds. The evidence should be unforgeable and should assure that the server will not act against the client's interest. Remote attestation provides such evidence by allowing clients to accurately verify if the remote server's state is compromised. A server can be trusted if the client can accurately verify all the software binaries that the server has executed [9].

The veracity of software is established through its identity, which is expressed by means of the hash1 of the software binary. For verification of the server's state, the measured hash of all the software binaries (measurement list) is sent to the client. The client performs the comparison against known software hash values, whose security has been verified. This will enable clients to verify that the server is free of malware or any unauthorized software. Remote attestation [9] refers to the process of authenticating and verifying the state of the remote platform and its operating system outside of the platform.

The remote platform can either be hosted on a physical server or a Virtual Machine (VM) in the physical server or both. In the context of cloud computing, remote attestation of the cloud server is performed either by cloud clients or a trusted third party on behalf of the cloud clients. Based on remote attestation, trusted computing technology was developed by the Trusted Computing Group (TCG). It provides specifications for securely reporting and verifying a remote platform (i.e., server hardware and software).

Existing research work in remote attestation of the server includes: securely collecting and storing information about the software state (hash values) of the server

[9], methods for using the information on the state locally in the server [10], for conveying the state information to an external client for remote attestation [11] and for managing the list of software that is allowed to be executed in the server.

This research paper focused on architectures [12] that enable secure transactions between cloud clients and untrusted providers. We studied the feasibility of this architecture in a real-world system using a Privacy Enhancing Technology (PET). We further investigated the limitations of PET and how Trusted Computing architectures (remote attestation) can be used to address these limitations. We identified issues with state of the art in remote attestation architectures and proposed improvements to it. Finally, we introduced the concept of subjective and dynamic trust in the cloud computing context

5.4.3 IMPORTANCE OF BLOCKCHAIN TECHNOLOGY

Blockchain technology is currently the most significant topic in the IT industry. In the last couple of years, Blockchain has made the headlines in business and technology news, as business leaders continue to admire the success stories of cryptocurrency and smart contracts [16].

Despite the common notion that Blockchain technology is virtually impossible to hack, the Blockchain system has been subject to numerous cyber attacks in recent years. Two years back, more than 10 percent of all cyberattacks in the world targeted Blockchain systems [17]. Further, the annual growth rate of hacking incidents and their loss against Blockchain systems surpass all other types of IT systems during their technology maturity periods. Some IT specialists consider these phenomena as a natural pattern of cyber threats against emerging technologies because, as new technology becomes popular, the number of cyberattacks against that technology inherently increases. Many researchers also point out that most system implementations of Blockchain technology have been focused solely on the cryptocurrency industry, where huge financial transactions provide high monetary rewards to a hacker once a cyber-attack succeeds.

In researching numerous cyberattacks against Blockchain systems, one surprising theme emerged: despite the number of security incidents, most victims still believe the Blockchain system remains safe, sound, and secure. They looked outside the system for the root cause of the heists and the cyberattacks, such as human mistakes, programming errors, immature usage of technology.

A. Technically Blockchain Concept

For the exploration of technology, this section describes how Blockchain works from a high-level view. The main process in Blockchain is adding transaction records to a public ledger that lists past transactions. The collection of records is called a block. The public ledger of past transactions is called the Blockchain, as it is a chain of blocks. The Blockchain is responsible for verifying to the network that a transaction has occurred. A node (user) on the Blockchain network verifies the validity of the transaction and prevents attempts to misuse or alter legitimate data transactions. [17]

B. Simple Structure of Blockchain

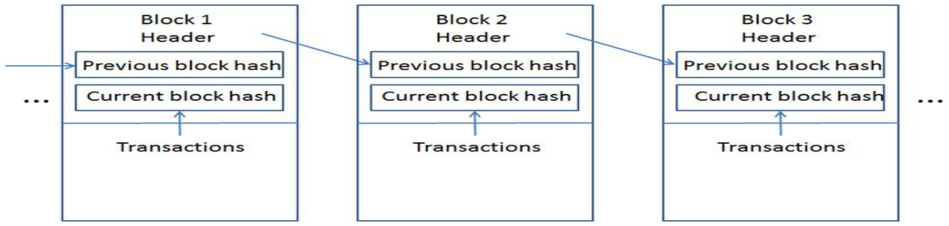


Figure 5:1 Simple Structure of Blockchain

As shown in figure 5.2, the process within Blockchain is divided into six phases: initial request of data transaction, initiation of new block creation, start mining, complete mining, validation of the new block, and chaining of the new block at the end.

C. Technology for Autonomous Data Management, But not for security

Blockchain is a technology for data management in the distributed system environment. The adoption of the technology aims to achieve fail-proof, infinite system operation that is self-fuelled without central intermediaries. That is, Blockchain technology is not designed to protect the entire system environment.

The use of this technology can securely store information in a decentralized system environment, but system security is not the ultimate goal of this technology.

For example, Blockchain's data security is maintained by the distribution of the same data to entire nodes.

The meaning of security in this way is limited within the inherent permanence and invariance. For instance, Blockchain cannot handle data that requires privacy, such as military classified data or corporate business secrets. Further, Blockchain cannot perform other data processing besides storage, such as modification and deletion. This indicates that separate security protections must be implemented to protect the rest of the data processing tasks other than Blockchain at the system level. Therefore, it is dangerous to assume that Blockchain can secure an entire system environment, making it invulnerable to outside cyberattacks. Even if the discussion about the technology was confined to the database domain, Blockchain is not superior to any centralized database in any aspect besides decentralization.

D. Blockchain System Security Domains

- *Threat Modelling:* Threat modelling is a common exercise conducted by most organizations to approach cyber threats more systematically and identify potential system security issues in advance [18]. In general, this threat exposes a system to cyberattacks attempting to steal transmitting data or eavesdrop on communication channels to identify theft, breaking into a secure channel, or interrupting user access. Threat modelling also discovered the cyber threat of data tampering, an act in which user-submitted data is changed to malicious data. In general, data tampering exposes a system to data manipulation causing incorrect or unintended system execution, including component tampering, data corruption, data manipulation, or ledger malleability that corrupts Blockchain protocol. Another cyber threat, denial of service, is a situation in which an authorized user's access to a computer network is interrupted with thirty-six malicious intent. Denial of service exposes public-internet-accessible system components to the cyberattacks of operation halt, system malfunction, or data corruption. A cyber threat of privilege escalation is also possible. Privilege escalation exposes centralized system components (such as Multi-Sig authentication or cryptocurrency exchange) to cyberattacks involving access control circumvention, system monitoring bypass, or third-party security solution break-ins. The cyber threat of data disclosure is also in system components designed to process or store sensitive data such as cold/hot wallets and online/offline storage. In general, data disclosure includes security risks like data loss or data theft. A cyber threat of broken non-repudiation occurs in the distributed application (dApps) such as smart contracts. In general, this threat includes security risks such as bypassing security logic, re-entry, or race condition within source code or consensus protocol manipulation[19].

- *Four Security Domains of Blockchain System:* A platform domain (D-1) mainly includes Blockchain elements such as nodes (users) and shared data (public ledgers). Since a consensus of all nodes reviews data validation and decides on block addition, nodes (users) are considered the most important components in a Blockchain system. Ledgers are the data in the system stored at each node. In this domain (D-1), a security review is mainly focused on redundancy, synchronization, and communication for ledger (data) processing. A front-end domain (D-2) includes a front-end facing server and an application such as a web server for a digital wallet or third-party security solution, cryptocurrency exchange servers, and online-based cold/hot storage. This is the same or very similar to the prevalent centralized IT system environment. A distributed application thirty-eight decentralized application (dApps) domain, (D-3) includes mostly proprietary applications that run based on Blockchain. Unlike conventional and existing computer applications, the dApps are not isolated within web servers or personal workstations but shared across the entire Blockchain system environment. Hence, security evaluation in this domain should be considered from the aspects of static (source code-based) and also dynamic (running and execution cases). The end-points domain (D-4) includes terminals, computers, or even mobile devices through which users communicate with a Blockchain system for usage and services. Data is entered as an input, sent as a request, and produced as an output in this domain, considered the most vulnerable area in a data flow chain. This domain will be the optimum target area for a potential attacker, so it requires effective protection in the end-user environment from malware attacks against personal computing devices, Cross-Site Scripting attacks, or Cross-Site Request Forgery attacks against client web browsers or computer virus infections [20].

5.5 LITERATURE SURVEY ON NATIONAL & INTERNATIONAL SCENARIO: PROPOSED SYSTEM

Enterprise businesses are being transformed to meet the evolving challenges of today's global business economy. New innovations and new business models are enabling new kinds of productivity, competitive advantage, revenue growth, and efficiency that drive the top line and the bottom line. Security is fundamental to the ability to leverage, with confidence, these rich services that are critical to business success. The comprehensive and diverse security portfolio enables the complex security challenges faced in this environment to be addressed through an integrated, defence-in-depth approach to security that is embedded in end-to-end solution architectures. In the proposed system, the Network Security Integration solution describes how to extend this integrated, defence-in-depth approach to security to encompass the mobility services offered by a LAN. Mobility is a critical service for enterprises, offering employees greater flexibility, and enabling increased productivity, through pervasive access to network resources and applications. However, this service offering must comply with the defined network security policies and integrate with the end-to-end network security strategies in order to be compliant, effective, and efficient. Network Security is an ongoing process of defining security policies, implementing proactive security measures to enforce them, monitoring the network to obtain visibility into activity, identifying and correlating anomalies, mitigating threats and reviewing what occurred in order to modify and improve the security posture.

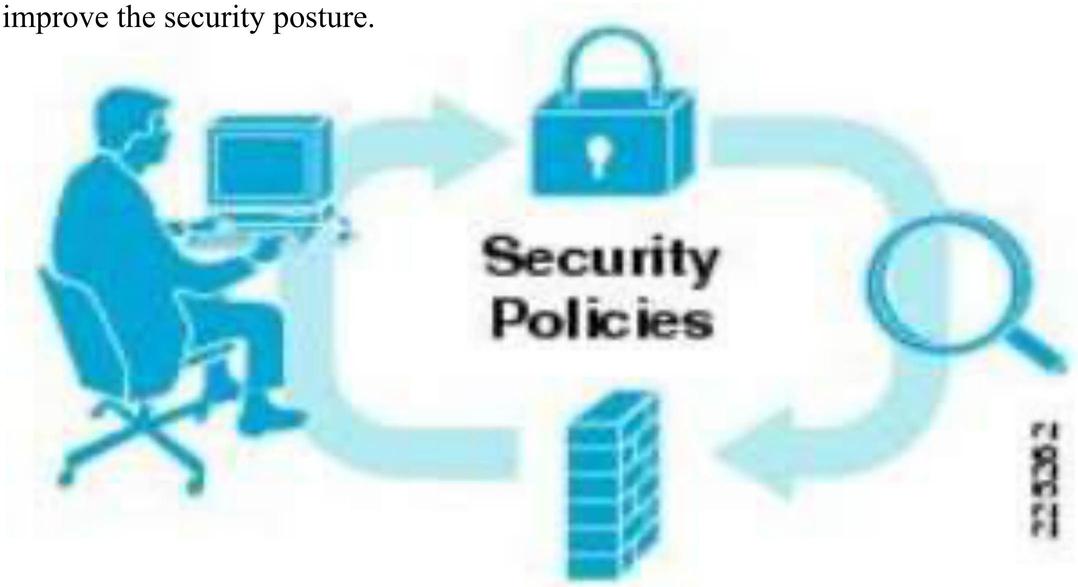


Figure 5:2 Security Policies

A wired or wireless network is only one of the attack vectors against a network. While a WLAN network must be secure and able to protect itself from attack, a network-wide security solution that only addresses WLAN-related attacks is dangerously unbalanced. Mobile network clients need to be protected on all interfaces at all locations, enterprise networks need to be protected on all their perimeters, and monitoring and anomaly detection are required regardless of the source of network traffic. Ideally, the same sets of tools and interfaces should be used to provide these baseline security functions as it reduces operational costs, reduces the risk of misconfiguration, and avoids the creation of an unbalanced security architecture that can be simply bypassed.

5.5.1 Security Solution Components

The Secure Wireless Architecture is built on the core architectures for the branch and campus networks. The Secure Network Architecture describes the integration and collaboration of security solutions with the Unified Networks to provide a common security framework for networks regardless of the client access mechanism. The core components of the Secure Architecture includes Unified Network, Intrusion prevention, Rogue detection and mitigation, Access control, Traffic encryption, User authentication, RF interference, and DoS monitoring, Security vulnerability monitoring and auditing, Infrastructure hardening—MFP, infrastructure device authentication, CSA, NAC appliance, Firewalls, IPS, MARS.

5.5.2 Solution Architecture

The purpose of the Secure Network Solution Architecture is to provide common security services across the network for wireless and wired users and enable collaboration between wireless and network security infrastructure for layered security architecture. This architecture is equally applicable in both campus and department deployments. The core components of this architecture are:

- Unified Network Architecture
- Campus
  Architecture
- Department Architecture

The Unified Network Architecture provides the core mobility services platform securing the wireless environment as well as all the functions required to secure the wireless deployment itself. The underlying campus and department architectures provide a secure high performance, high availability network platform for mobility services. This provides a common wired and wireless platform for the integration of security services, allowing common security architecture to be developed for all network clients and traffic types.

Security Elements and General Network Security Elements		
Proactive Security	WLAN Specific Elements	General Network Security Elements
Harden the network infrastructure	Cisco Unified Wireless Network, LWAPP, Management Frame Protection, 802.1X	Infrastructure Hardening
Protect the Endpoints	Wi-Fi protected Access / Wi-Fi protected Access 2	CSA / Cisco Secure Services
Identify and Enforce policy on users	Wi-Fi protected Access/ Wi-Fi protected Access 2 Client	CSA, Cisco Secure Services, NAC and Cisco Firewall
	Exclusion on the Wireless LAN Controller	
Secure Communication	Wi Fi protected Access / Wi-Fi protected Access 2	
Access Control	Access Control Lists on Wireless LAN Controller	Cisco Firewall
Operational Security		
Monitor the network	Wireless LAN Controller, Wireless Control System, Adaptive Wireless IPS	AAA, SNMP, Platform Management and CS-MARS
Detect and Correlate anomalies, mitigate	Wireless LAN Controller, Control System, Adaptive	CS-MARS, CSA,IPS

threats,	Wireless IPS	

Table 5-1 Security Elements and General Network Security Elements

5.5.3 Unified Network System

WLANs in the enterprise has emerged as one of the most effective means of connecting to a network. The network is a unified wired and wireless network solution that addresses the wireless network security, deployment, management, and control aspects of deploying a wireless network. It combines the best elements of wireless and wired networking to deliver secure, scalable networks with a low total cost of ownership. Client devices, Access points, Controllers, network management, and mobility services work together to deliver a unified enterprise-class solution.

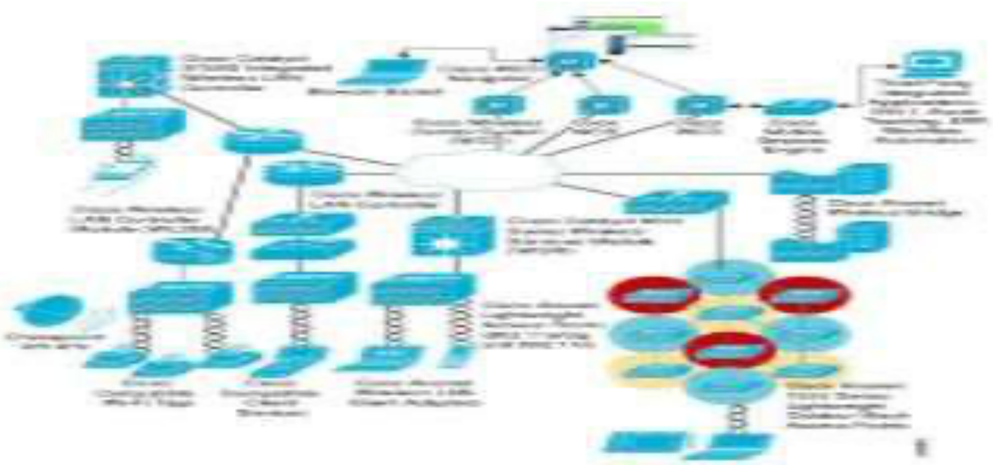


Figure 5:3 Unified Network infrastructure

The components required for secure deployment and operations of a wireless network are built into the Cisco Unified Network infrastructure. Leveraging Wireless LAN controllers, access points, and wireless management systems provide comprehensive wireless security, reducing capital costs while streamlining security operations. Leveraging the features and functions of our proposed network security portfolio delivers a greater degree of control over wired and wireless networks, users, and their traffic. Further, supplementing wireless security with wired network security provides layered defences that deliver more thorough protection, with greater accuracy and operational efficiency for both network operations and security operations teams within the departments. Wireless, it's over the air transmission, has unique security requirements. The primary security concerns for a network are:

Rogue access points and clients that can create backdoor access
to the network. Hacker access points, such as evil twins and
honey pots

Denial of service that disrupts the network.

Network and traffic cracking.

Controlling the users of the network connect to, especially when they are
outside of the organization—security for guest users.

Security event management and reporting on all of these functions, complete with physical location tracking of where the security event took place on the network, is key to any robust security solution. All of these concerns are addressed by security technologies built-in in the controllers, access points, and CS management system. The same gear that provides connectivity to users also provides security for the entire deployment. A built-in intrusion prevention system detects and mitigates rogue access points and clients, as well as DoS attacks, hacker access points, network reconnaissance, eavesdropping, and attempted authentication and encryption cracking. Further, it can provide wireless IPS monitoring from the same access points that service user traffic, as well as provide full-time dedicated wireless IPS monitoring. Providing both approaches enables site-specific flexibility based on network security policies, which reduces the high infrastructure costs associated with stand-alone wireless intrusion prevention systems. Networks should be self-defending. Providing a hardened network core that is impenetrable to attacks is better than simply detecting an attack after the damage is done. Secure guest access management is also addressed in the Unified Network infrastructure, providing captive guest user portal, network segmentation, and full guest management functionality. Finally, wrapping all this together is the Security management system.

5.5.4 Secure Wireless Architecture

The Secure Wireless Solution Architecture consists of a WLAN security component and network security components. The Cisco Unified Wireless Network provides the WLAN security core that integrates with other Cisco network security components to provide a complete solution. The Cisco Unified Wireless Network Architecture provides a mechanism to tunnel client traffic to the wireless LAN controller in a campus service block. The services block provides a centralized location for applying network security services and policies such as NAC, IPS, or firewall. In addition to the components protecting the network in the services block, the Cisco Security Agent provides an additional protection network, as well as protecting the mobile client. Wired/wireless collaboration does not just mean putting more boxes in the network. It is the purpose-built linkages that have been built between Cisco's wired and wireless security technologies to deliver a superset of security functionality and protection.

5.5.5 Campus Architecture

The overall campus architecture is more than the fundamental hierarchical router and switch design. While hierarchies such as access, distribution, and core are fundamental to how to design and build campus networks, they do not address the underlying questions about what a campus network does. The campus network provides services that are used to build secure wireless solutions. Services such as these provide the foundations for the Secure Solution are High availability, Access services, Application optimization, and protection services, Virtualization services, Security services, and operational and management services.

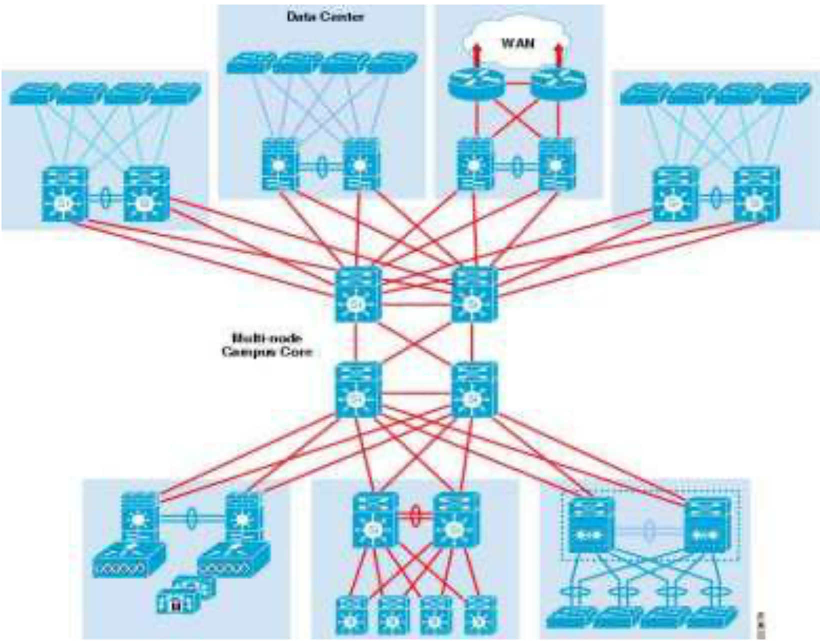


Figure 5:4 Campus Architecture

5.5.6 Department Architecture

The full-service branch provides the same solutions and services to a branch as are available for the campus. This includes security and wireless, and the Secure Wireless solution is equally applicable for department deployments as it is for the campus. There are a number of LAN/WLAN, firewall, and NAC options for a department, including an H-REAP, WLAN Controller Module (WLCM), 21XX WLC, or larger WLCs, PIX, ASA, or IOS Firewalls, NAC appliances, and IPS appliances

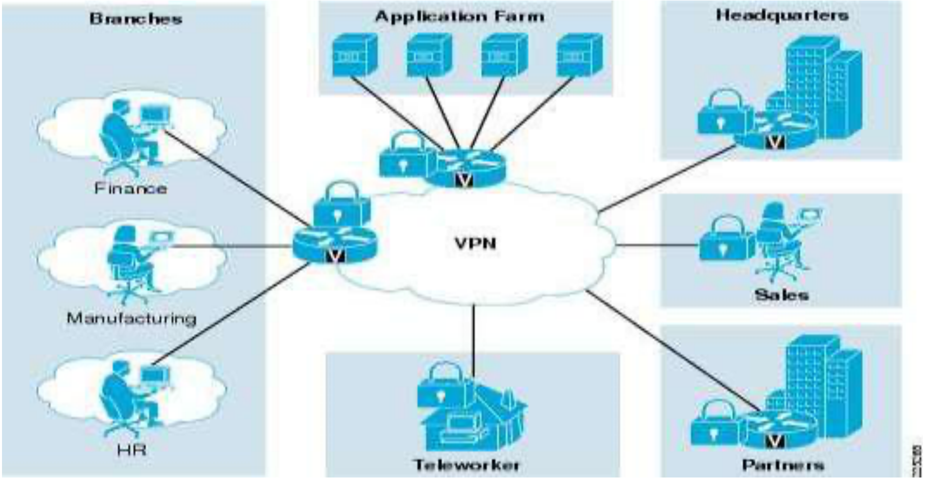


Figure 5:5 Department Architecture

References:

1. Investigation On The cloud Computing Security Using PET and Remote Attestation In Cloud Architectures by Dr.K.Sai Manoj published in International Journal of Current Advanced Research Volume 8; Issue 10 (D); October 2019 http://dx.doi.org/10.24327/ijcar.2019 Impact Factor: 6.614 ISSN: O: 2319-6475, ISSN: P: 2319-6505; October 2019http://journalijcar.org/issues/investigation-cloud-computing-security-using-pet-and-remote-attestation-cloud-architectures.
2. GW Van Blarkom, J J Borking, and JGE Olk. Handbook of privacy and privacy-enhancing technologies. Privacy Incorporated Software Agent (PISA) Consortium, The Hague, 2003.
3. Keith Frikken and Mikhail Atallah. Privacy-Preserving Cryptographic Protocols. In Digital Privacy, pages 47–69. Auerbach Publications, November 2009.

4. Shafi Goldwasser and Silvio Micali. Probabilistic encryption and how to play mental poker, keeping secret all partial information. In Proceedings of the fourteenth annual ACM symposium on Theory of Computing, pages 365-377, New York, NY, USA, 1982. ACM.

5. Craig Gentry. A fully homomorphic encryption scheme. Ph.D. thesis, Stanford University, 2009.

6. Qin Liu, Guojun Wang, and Jie Wu. An Efficient Privacy-Preserving Keyword Search Scheme in Cloud Computing. Computational Science and Engineering, 2009. CSE '09. International Conference on, 2:715-720, August 2009.

7. Karthick Ramachandran, Hanan Lutfiyya, and Mark Perry. Chaavi: A Privacy-Preserving architecture for Webmail Systems. In Cloud Computing 2011, The Second International Conference on Cloud Computing, GRIDs, and Virtualization, page 133 to 140

8. Daniele Micciancio. The first glimpse of cryptography's Holy Grail. Communications of the ACM, 53(3):96–96, March 2010

9. Morrie Gasser, Andy Goldstein, Charlie Kaufman, and Butler Lampson. The Digital distributed system security architecture. In Proceedings of the 1989 National Computer Security Conference, pages 305-319, 1989

10. S Bajikar. Trusted platform module (TPM) based security on notebook pcs-white paper. White Paper, Mobile Platforms Group-Intel Corporation, 20, 2002.

11. B Bertholon, S Barrette, and P Bouvry. Certicloud: A novel tpm-based approach to ensure cloud iaas security. Cloud Computing (CLOUD), 2011

12. Conceptual oriented study on the cloud computing architecture for the full Security Dr.K.Sai Manoj *International Journal of Engineering and Technology*, Volume 7, Issue 4, 2018, Science Publishing Corporation

13. Investigations on the Cloud Data Storage Security-Based Using Diffie Hellman Algorithm Dr.K.Sai Manoj appreciated article in *International Journal of Computer Engineering and Applications*, Volume XIII, Issue VI, JUNE. 19, www.ijcea.com ISSN 23213469

14. Research on Security and Vulnerabilities of Blockchain Systems by Dr.K.Sai Manoj, published in the International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653;

IC Value: 45.98; SJ Impact Factor: 7.177 Volume 8 Issue I, Jan 2020 (Single author)https://www.ijraset.com/fileserve.php?FID=26233.

15. Rosic, "blockgeeks.com," 2016. [Online]. Available: https://blockgeeks.com/guides/what-is-blockchain-technology/. [Accessed 21 03 2018].
16. T. R. N. Desk, "Why is Blockchain Gaining Popularity?" 31 May 2017. [Online]. Available: https://www.readitquik.com/articles/digital-transformation/why-isblockchain-gaining-popularity/. [Accessed 21 12 2017]
17. B. Wiki, "Mining," Bitcoin Wiki, [Online]. Available: https://en.bitcoin.it/wiki/Mining. [Accessed 1 12 2018].
18. L. Turvey, "Blockchain Implementation Security. A hardening how-to," 22 8 2017. [Online]. Available: https://www.pentestpartners.com/security-blog/blockchainimplementation-security-a-hardening-how-to/. [Accessed 14 3 2018].
19. Conceptual oriented study on the cloud computing architecture for the full Security Dr.K.Sai Manoj International Journal of Engineering and Technology, Volume 7, Issue 4,2018, Science Publishing Corporation.

20. INVESTIGATIONS ON THE CLOUD DATA STORAGE SECURITY BASED USING DIFFIE HELLMAN ALGORITHM Dr.K.Sai Manoj appreciated article in International Journal of Computer Engineering and Applications, Volume XIII, Issue VI, JUNE. 19, www.ijcea.com ISSN 23213469
21. Dimitra A. G. (2017) Security Policies for Cloud Computing, 26 Jan 2019 [Online] Available:https://www.dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/11007/Georgiou_Dimitra.pdf?
22. Muijnck-Hughes Jan de (2011) *Data Protection in the cloud,* 12 Jan 2019 [Online], Available: http://www.ru.nl/ds
23. Venkata S. et al. (2011) *Security Techniques for Protecting Data in Cloud Computing*, 12 Jan 2019 [Online] Available: https://www.bth.se/com
24. Ali Asghary K. (2011) *Security Analysis and Framework of Cloud Computing with Parity-Based Partially Distributed File System*, 26, Jan

2019 [Online] Available; https://www.academia.edu/27767213/security_Analysis_and_Framework_of_cloud_computing_with_Parity_Based_Partially_Distributed_File_System

25. Nabil Giweli (2013) *Enhancing Cloud Computing Security and Privacy*, 20, Jan 2019 [Online]Available:https://www.researchdirect.westernsydney.edu.au/islandora/object/uws%3AI7310/.../view

26. Zhou Miao (2013)*Data Security and Integrity in cloud computing*, Doctor of Philosophy thesis, School of Computer Science and Software Engineering, University of Wollongong. http://www.ro.uow.edu.au/thesis/3990

27. Sudhansu R. L. et al. *Enhancing Data Security in Cloud Computing Using RSA Encryption and MD5 Algorithm*, International Journal of Computer Science Trends and Technology (IJCST) – Volume 2, Issue 3, June 2014

28. Aastha Mishra (2014) *Data Security in Cloud Computing Based on Advanced Secret Sharing Key Management System*, 20 Jan 2019 [Online] Available: https://www.ethesis.nitrkl.ac.in/5845/1/212CS2110.pdf

29. NesrineKaaniche (2014) *Cloud Data Security based on Cryptographic Mechanisms*, 26 Jan 2019 [Online] Available: https://www.tel.archives-ouvertes.fr/tel-01146029/document

30. Afnan U.K. (2014) Data Confidentiality and Risk Management in Cloud Computing 2 Feb 2019 [Online]Available:https://www.ethesis.whiterose.ac.uk/13677/1/Thesis_Final_Afnan _27072016_ EngD.pdf

Chapter 6

6 Chapter 6 : Analysis of Cloud Computing

6.1 Methodology

According to our literature review, we found that Mobile Cloud Computing ICN is an evolving paradigm that gives the ability to cache content as near as possible to user and provides better mobility support than previous environments. To the best of my knowledge there is limited work done before on the issue of group mobility in 5G- Mobile Cloud Computing ICN environments. We will propose a novel approach in which we will exploit group mobility of users as well as the popularity of videos that will reduce traffic at backhaul and decrease retrieval delay time of videos by leveraging 5G- Mobile Cloud Computing ICN architecture.

Optimization Method :

In my Optimization on 5G SDN approach in order to route the requests to the proper MCC server instance. 5G SDN organized by routing information based on the content offloading. The advantages of 5G SDN for Cloud computing services have been presented in works. In our case, the MCC server Optimization scheme messaging to communicate final devices with the structure. Therefore, the transport is delegated to web Application. To unload the 5G SDN controller from that burden, web Application proxies are collocated at the MCC servers, proactive 5G SDN the deployment of specific caching software. Te adopted approach relies on already routing is performed to direct requests to the nearest proxy from the 5G SDN controller entry point. An equivalent approach is presented in. 5G SDN controller is deployed on the same MCC server instance as the proxy and near to the 5G SDN entry points. The instance decides the Optimization unit to which the request will be directed and programs the path to that MCC server. The 5G SDN controller installs the flows to redirect the request from the proxy to the proper Optimization unit which is in the same MCC server instance in this case. When the Optimization unit calculates the fix, the result is returned through the proxy to the user . (ii) Te second request is a user searching request, indicated as location. User, which is issued by an external application. This request arrives directly to the nearest web Application proxy. (iii) When the UE change to another AN , requests are addressed to a different local MCC server to compute the location as above . Notifications of user Optimization from intelligent infrastructures are not included. The 5G SDN controller redirects the requests to the nearest MCC server instance's web Application proxy of the last user's known Optimization. For the moment, our implementation routes the request to the nearest Optimization unit to the entry web Application proxy, with the aim of reducing the response delay

6.2 Security Analysis & Metrics Consideration:

On the sequence of URL naming followed by hierarchal naming, which consists of many components. The routing performance will be done through name-based contents to deliver subscribers. The Cache Pollution attack is vulnerable to different method which filled the corrupted files in the cache system. Contrary most of the time, the cache pollution attack could not be monitored where the attack is in progress or not. The communication system denies the services from routers which indicates the attacks occurred even then communication is happening through routers. We have proposed the DES Cache System (Discrete Event Simulator) measure experimental cache parameters through the policies Least Frequency Used, Least Recently, Variable Data Used, and Multiple attacker Behaviors. The number of attackers will send unpopular request files from different ISP must pollute the nearby nodes which affect regular consumer nodes through a standard request from Router cache. Usually name based router will attain an 85% to 90% hit ratio and the client's standard request entry will be 1Mbyte. Consider a typical internet architecture using Link rate is 1Gbps,data access rate between the communication 100 Mbps and Cache size is 100Gbytes. The normal detection scheme will access the subscriber communication data ranges and identify the security services and unique network attributes.

Since we have been introduced Constant Interval Frequency Used Policy that would provide a time frame for access link delay connecting the routers and subscribers through this Constant Interval, we could have to find the attacks.

Optimization Method :

Our Optimization on 5G SDN approach to route the requests to the proper MCC server instance. 5G SDN organized by routing information based on the content offloading. The advantages of 5G SDN for Cloud computing services have been presented in works. In our case, the MCC server Optimization scheme messaging to communication terminal devices with the structure. Therefore, the transport is delegated to web Application. To unload the 5G SDN controller from that burden, web Application proxies are collocated at the MCC servers, proactive 5G SDN the deployment of specific caching software. Te adopted approach relies on already routing is performed to direct requests to the nearest proxy from the 5G SDN controller entry point. An equivalent method is presented in. 5G SDN controller is deployed on the same MCC server instance as the proxy and near to the 5G SDN entry points. The situation decides the Optimization unit to which the request will be directed and programs the path to that MCC server. The 5G SDN controller installs the flows to redirect the request from the proxy to the proper Optimization unit which is in the same MCC server instance in this case. When the Optimization unit calculates the fix, the result is returned through the proxy to the user . (ii) Te second request is a user searching request, indicated as location. User, which is issued by an external application. This request arrives directly to the nearest web Application proxy. (iii) When the UE change to another AN , requests are addressed to a different local MCC server to compute the location as above . Notifications of user Optimization from intelligent infrastructures are not included. The 5G SDN controller redirects the requests to the nearest MCC server instance's web Application proxy of the last user's known Optimization. For the moment, our implementation routes the request to the nearest Optimization unit to the entry web Application proxy, with the aim of reducing the response delay

6.3 Service Cache and Task offloading in MCC Mathematical Model:

Optional Server Energy required to complete a computing Cycle.

O=k(f*f) ---(1)

For local server task computing, the Local Server computing time is calculated by the following mathematical model

$L^{l}_{n,k} = \frac{\omega_k}{f^{l}_{n}}$ --(2)

Here n represents the number of service cache Task offloading, and K represents number of tasks n={1,2,....N} and k={1,2,3........K}

Optional Server required to complete a local task is represented as

OP=$K(f_n^l) * (f_n^l)\omega_k$ ---(3)

No of Task required to service cache to complete the k task is given by

$S_{n,k} = x_k \frac{\omega_k}{f_n^c} + (1 - x_k)\left[\alpha_n L^l_{n,k} + (1 - \alpha_n) T^c_{n,k}\right]$ -----------------------------(4)

α_n is the task offloading process

And the corresponding cache can be calculated by

$C_{n,k} = (1 - x_k)\left[\alpha_n L^l_{n,k} + (1 - \alpha_n) E^c_{n,k}\right]$ --(5)

we are considering the following constrains

$T1{:}\sum_{k=1}^{k} x_k s_k \le C_e$

$T2{:}\sum_{n=1}^{n} \alpha_n f_n \le C_s$

$T3{:}T_{n,k} \le D_n, \forall n \in N, \forall k \in K$

$T4{:}x_k \in \{0,1\}, \forall k \in K$

$T5{:}\alpha_n \in [0,1], \forall n \in N$

The constrains above are

1. Initial condition (T1) represents that the total size of cached computing task never cross the Mobile Cloud Computing capacity.

2. The Task (T2) ensures the total computation required resources for the offloaded task should not exceed the Mobile computation capacity of the Cloud.

3. The next Task (T3) shows that the offloading task performance for user *n* is successful before ends the lifetime.

4. The Task (T4) ensures that the service cache is a binary variable.

5. Final Task (T5) is split the task.

The capacity with respect to α_n the function is represented as below

$f(\alpha) = \sum_{n=1}^{N} (1 - x_k^0)[\alpha_n E^l_{n,k} + (1 - \alpha_n) T^c_{n,k}]$ -------------------------------(6)

And Mobile Cloud computing is done with respect to alpha is given by

$Minimize\ f(\alpha) with\ respect\ to\ \sum_{n=1}^{N} \alpha_n f_n^c \leq c_s$

$T_{n,k} \leq D_n, \forall n \in N, \forall k \in K$

$\alpha_n \in [0,1], \forall n \in N$ --(7)

To do the service cache task following Mobile Cloud Computing inefficient way we follow the task caching process

 in the above function. We performed task offloading and now we are going to do task caching and now α is replaced by α*.

$K(x) = \sum_{n=1}^{N}(1 - x_k)[\alpha_n^* E_{n,k}^{l} + (1 - \alpha_n^*)T_{n,k}^c]$ ------------------------------ (8)

A further concept is focus on the offloading method.

$Minimize\ K(x) with\ respect\ to\ \sum_{n=1}^{N} \alpha_n f_n^c \leq d_s$

$T_{n,k} \leq D_n, \forall n \in N, \forall k \in K$

$x_k \in [0,1], \forall k \in K$ --(9)

We are using a totally ten service stations and the total capacity or the total number of services is 120. In the simulation, we will set up 10 base stations, and the base station communicates with the UE.

6.4 Technical Concept

Mobility prediction has been one of the critical challenges in Mobile Cloud Computing. Many kinds of research in the last generations (3G and 4G) networks had done on mobility, but their methods only focused on predicting mobile node patterns but not on caching the content. While Mobile Cloud Computing ICN decouples the content from Cloud Computing, So the paradigm provides secure access from the nearest access point rather than typical IP based retrieval from cloud computing content provider; therefore, Mobile Cloud Computing ICN can provide better mobility support. Mobility has been considered in Mobile Cloud Computing ICN by many researchers such as [4][9], but these works only focused on individual mobile nodes pattern. Some tasks like [11][12] also considered mobility under the Mobile Cloud Computing ICN environment. Their works were in Cloud and device to device.

The conclusion of their research is how to cache the content on mobile cloud computing and how to retrieve content from Mobile Cloud.

6.4.1 Group Mobility Model

Spatial locality (SL) and Temporal locality (TL) are group mobility metrics. SL can give information about speed and direction. Similar users are moving at the same rate on a similar path.TL will provide a similar user at a given time slot existing at the same location. While combing both will provide us with a complete set of information location and direction from which observation about group mobility can easily extract. Dual locality Ratio (DLR) combines SL and TL and investigates group mobility impact on network performance, and the following is the equation for DLR.

$$DLR_{ij} = (1-\gamma_{DLR})\left(\frac{1}{1+\sqrt{\left(\frac{d_{ij}}{d_{max}}\right)^2+\left(\frac{s_{ij}}{2s_{max}}\right)^2}}\right)+\gamma_{DLR}\left(1-JSD_{ij}\right) \quad (1)$$

$d_{ij}$is the euclidean distance between user i and j where $d_{max}$is the transmission range and $s_{ij}$is the relative velocity vector between user i and j, $s_{max}$is the total speed that the network can track. JSD_{ij} is for finding TL and γ_{DLR} is a tuning parameter.

6.4.2 Popularity model

For the prediction of popular videos, we will use Zipf[18] distribution, and the following is the equation.

$$p_{v_f} = \frac{f^{-\propto}}{\sum_{j=1}^{F} j^{-\alpha}} \quad (2)$$

It will calculate the frequency of how many times the video *f* is requested if the frequency is more significant than other videos that video will be considered popular and cached.

6.4.3 Different Preference videos

A group will have different preferences member to for the following is the equation.

$$up_{i,f} = p_{vf}\left(\frac{m(C_i,D_f)}{\sum_{K=1}^{M}(C_k,D_f)}\right) \quad (3)$$

In each time slot, the user can prefer a file *f*in the above equation can calculate a group.

6.5 Evaluation Metrics

6.5.1 Average retrieval delay

We will use this metric to evaluate how much faster a user can fetch the requested video. QoE can be affected if the average retrieval delay is high. The average retrieval delay RD can be calculated by the following equation (4).

$$RD = \frac{\sum r_i}{N} \qquad (4)$$

6.5.2 Average Number of Choppy playback Time

By using this metric, we can observe the QoE of a mobile user. Each time when a handoff occurs which will lead to retransmission of packet due to lost packet if the newly connected content router or base station does not cache the video. Following is the equation for calculating the average number of choppy playback time.

$$CP = \frac{\sum p_i}{N} \qquad (5)$$

6.5.3 Average miss ratio

We will use the average miss ratio to calculate the efficiency of the proposed 5G-MOBILE CLOUD COMPUTING ICN approach. Following is the equation for calculating the average miss ratio.

$$MR = \frac{\sum m_i}{N}$$

References:

1. Armstrong, L.E., Hydration appraisal strategies. Sustenance opinions, 2005. Sixty-three (6): p. S40-S54.

2. Oppliger, R.A., et al., Accuracy of pee express gravity and osmolality as markers of hydration repute. Typical magazine of game nutrients and exercising Metabolism, 2005. 15(three): p. 236-251.

3. Manz, F., Hydration, and disorder. Diary of the yank university of nutrients, 2007. 26(suppl five):p. 535S-541S.

4. Manz, F. Furthermore, A. Wentz, The significance of correct hydration for the anticipation of ceaseless maladies.Sustenance reviews, 2005. Sixty 3: p. S2-S5.

5. Nidhibhatla and Kiran Jyoti, "An analysis of coronary heart ailment Prediction making use of different records Mining strategies", the worldwide magazine of Engineering research and generation (IJERT), ISSN: 2278-0181, Vol. One difficulty 8, October – 2012

6. Abhishektaneja, heart sickness Prediction machine using records Mining techniques, orientallogical Publishing Co., India, 2013.

7. Rashedur M. Rahman, farhanaafroz, assessment of numerous category strategies using distinctive statistics Mining tools for Diabetesdetermination, journal of software program Engineering and packages, 2013.

8. Nidhibhatlakiranjyoti, An analysis of heart disease Prediction making use of different facts Mining strategies, international journal of Engineering research and generation (IJERT), 2012.

9. Humarkahramanli, novruzallahverdi, design of a half breed framework for diabetes and coronary heart infections, Elsevier, 2008.

10. Marcel A.J. Van Gerven, Predicting coronary carcinoid infection with the loud limit classifier, Elsevier, 2007.

11. Mohammad Taha Khan, Dr. Shamimulqamar and Laurent F. Massin, A Prototype of

12. Malignancy/heart sickness Prediction version using records Mining, a global magazine of carried out Engineering research, 2012

13. M.Akhiljabbar, Dr.Priti Chandra, Dr.B.ldeekshatulu, coronary heart disorder Prediction gadget using

14. Conceptually based on the Data Mining Techniques for the Prediction of Hydration Assessment, Breath Analysis, and Heart Disease International

Journal of Innovative Technology and Exploring Engineering (IJITEE). Dr.K.Sai Manoj ISSN: 2278-3075, Volume-8 Issue-12S2, October 2019 http://www.ijitee.org/wp-content/uploads/papers/v8i12S2/L107510812S219.pdf (Single Author)

15. Countrywide Institute of Standards and technology, structures, ―manual for developing protection plans for federal facts structures‖, Vol. 800-18, February 2006, [Online]. To be had from: http://csrc.Nist.Gov/guides/nistpubs/800-18-Rev1/sp800- 18-Rev1-very last.Pdf/, [accessed December 2013]. [2] Divers S. - SANS Institute, "information safety coverage A development manual for huge and small businesses", November 2007, pp. Forty three-forty four.

16. Svantesson D. And Clarke R., ―privateness and client dangers in Cloud Computing", computer regulation and protection assessment, Vol. 26, 2010, pp. 391-397

17. Kshetri, N., ―privacy and protection issues in Cloud Computing: the area of establishments and institutional evolution‖. 2012, Bryan college of business agency and Economics, The Univ. Of North Carolina at Greensboro, NC27402-6165, us

18. national institute of standards and era."The NIST Definition of Cloud Computing" (PDF), September 2011. [Online].To be had from https://csrc.Nist.Gov/publications/element/sp/800-a hundred forty-five/very last, [accessed November 2013]

19. ECU network and facts safety organization (Enisa) ―Cloud Computing blessings, dangers, and tips for information protection‖, November 2009, [accessed June 2012]. [7] Arnold S., ―Cloud Computing and the issues of privateness‖, July 2009, KM global, pp.14-22

20. Whitepaper, A, ―organization Cloud Computing: transforming IT‖, Platform Computing, considered 13 March 2010, pp.6.

21. Xia Z., Zhu Y., solar X. And Chen L. (2014), "comfy semantic increase based are trying to find over encrypted cloud records helping similarity score "magazine of Cloud Computing‖, Springer three.1, pp. 1-

22. Kuyoro S.O., "Cloud Computing safety troubles and disturbing conditions", Proc. Worldwide mag of pc Networks (IJCN), 2011, vol. 3, problem:

23. Kavitha. And Subashini S.,–A survey on protection troubles in company transport fashions of cloud‖, global journal of community and computer applications, January 2011, vol. 34 difficulty 1, pp.1-11 [12] Robinson N., Valeri L., Cave J., Starkey T., Graux H., Creese S., Hopkins P.: The Cloud: knowledge the safety, privacy and receive as real with challenges. Organized for the Unit F.Five, Directorate- famous information Society and Media, ECU fee (2010)

24. Pallis, George. "Cloud Computing: the cutting-edge Frontier of internet Computing." IEEE net Computing 14.Five (2010): 70-seventy three. [Online]. To be had from http://cgi.Di.Uoa.Gr/~advert/M155/Papers/palisic10.Pdf, [accessed November 2012].

25. Securing the Cloud: A assessment of Cloud Computing, security Implications, and first-rate Practices‖. To be had from:http://www.Centurylinktechnology.Com/internet

26. Websites/default/documents/savvis_vmw_whitepaper_08 09.Pdf [accessed January 2013]. [15] Sans Institute, "An advent to Securing a Cloud surroundings‖, June 2012. [Online]. Available from: https://www.Sans.Org/analyzing- room/ whitepapers/cloud/advent-securing-cloud- environment34052 [accessed November 2012].

27. Cloud protection Alliance: –The notorious 9: Cloud Computing Top Threats in 2013‖. [Online]. To be had from http://www.Cloudsecurityalliance.Org/topthreats/, 2013 139

28. D. Lekkas, setting up and handling keep in mind within the public key infrastructure, laptop Communications 26

29. (16) (2003). G. Reese, Cloud application Architectures: building applications and infrastructure in the Cloud, in idea in exercising, O'Reilly Media, 2009.

30. B. Rajkumar, C. Yeo, S. Venugopal, S. Malpani, Cloud computing and developing IT systems: vision, hype, and fact for turning in computing due to the fact the 5th software program, destiny era laptop systems (2009) chance factors And safety troubles In various Cloud storage Operations

31. Dr.Good enough.Sai Manoj quantity- eight hassle-12, October 2019, ISSN: 2278-3075 (on- line) posted with the aid of Blue Eyes Intelligence Engineering & Sciences e-book (First author) (ELSEVIER Scopus)

32. Conceptual orientated research on the development of the Cloud records storage safety Dr.Ok.Sai Manoj international magazine of laptop technology developments and era (IJCST) – extent 7 problem 5, Sep-Oct 2019.

33. Cloud protection: hazard elements and safety problems in cutting-edge-day inclinations Dr.Good enough.SaiManoj international magazine of Engineering & technology, technological know-how Publishing business enterprise October 2019 (Scopus)

34. Research on the Security Policies for Cloud Computing International Journal of Innovative Technology and Exploring Engineering (IJITEE) Dr.K.Sai Manoj ISSN: 2278-3075, Volume- 8 Issue12, October 2019 (FirstAuthor) http://www.ijitee.org/wpcontent/uploads/papers/v8i12S2/L107610812S219.pdf

35. N. Calheiros, SLA-oriented aid Provisioning for Cloud Computing: challenges and solutions architecture 2011 global convention on Cloud Computing and administrations, from 1 to 10.2011.

36. Dejun Wang, An green model for Heterogeneous Cloud garage Cloud Infrastructure, magazine, 1877- 7058/10.1016,510-515,2011.

Rajkumar Buyya1,2, Saurabh Kumar Garg1, and Rodrigo

37. N. Calheiros, SLA-oriented aid Provisioning for Cloud Computing: challenges and solutions architecture 2011 global convention on Cloud Computing and administrations, from 1 to 10.2011.

38. Design and Development of Various Cloud Computing Architectures Improving the Security International Journal of Innovative Technology and Exploring Engineering (IJITEE) Dr.K.Sai Manoj ISSN: 2278-3075, Volume-8 Issue-12S2, October 2019 (First Author)

Chapter 7

7 Chapter 7 : Results and Discussion

I have proposed an advanced algorithm called advanced wheat stone algorithm. The data sensed from the devices is encrypted and stored in cloud and the key is shared with the receiver so that the receiver can decrypt the sensed data from the cloud. The third party cannot read the data from the cloud.

A smart caching mechanism used an edge environment over an Mobile Cloud Computing ICN architecture in which they used 1) Location prediction 2) Smart cache using machine learning method for the placement of mobile multimedia content on the edge nodes and at the end an smart cache replacement algorithm and there result showed that there proposed algorithms performed well against the comparative techniques which includes increased hit ratio and reduced access time.

I have proposed the DES Cache System (Discrete Event Simulator) measure experimental cache parameters through the policies Least Frequency Used, Least Recently, Variable Data Used and Multiple attacker Behaviors. The number attackers will send unpopular request files from different ISP must pollute the nearby nodes which affect regular consumer nodes through normal request from Router cache. Normally name based router will attain 85% to 90% hit ratio and the client normal request entry will be 1Mbyte ,Consider a normal internet architecture using Link rate is 1Gbps ,data access rate between the communication 100 Mbps and Cache size is 100Gbytes.The normal detection scheme will access the subscriber communication data ranges and identify the security services and network unique attributes.

In results we clearly did the comparison of exiting system with the proposed system on the following parameters.

- Packet Delivery Ratio
- End-to-end delay of the message transmitted

Simulation Results:

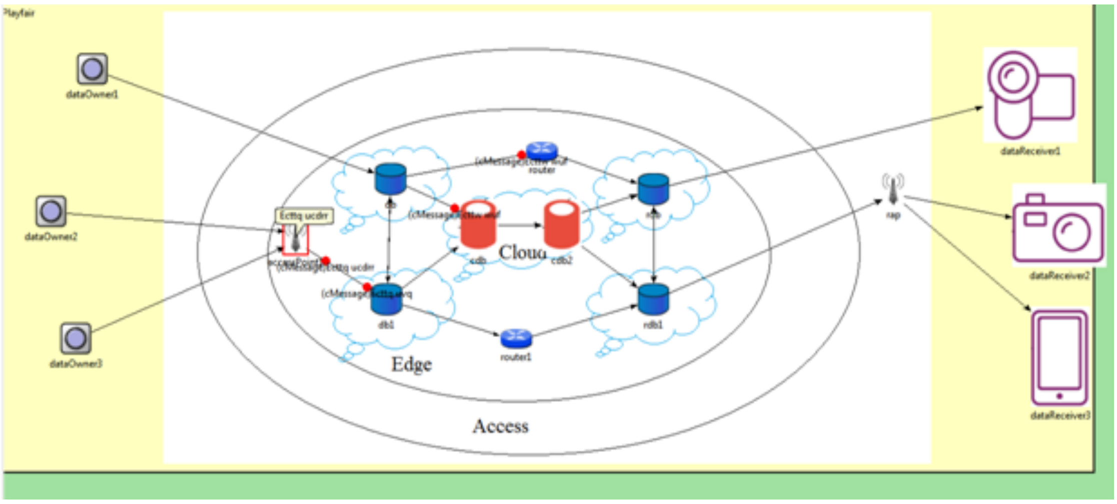


Figure 7:1 The figure depicts that the encrypted data is transferred from the access point to cloud's database. In cloud the data is stored in a central database (cdb)

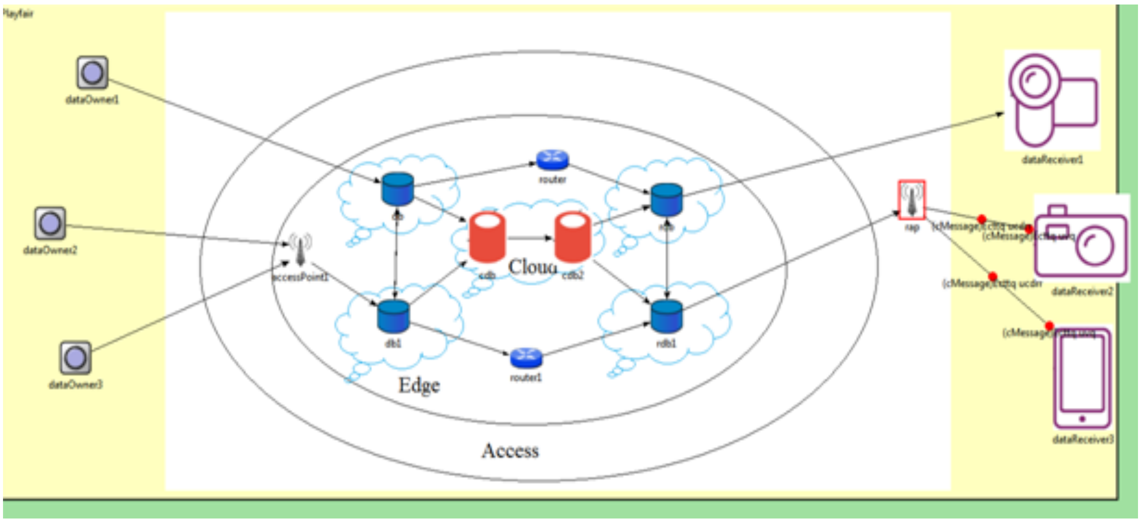


Figure 7:2 In the figure the data is transferred from receiver side access point to receiver. The receiver side equipment's like mobile phone , camera etc.

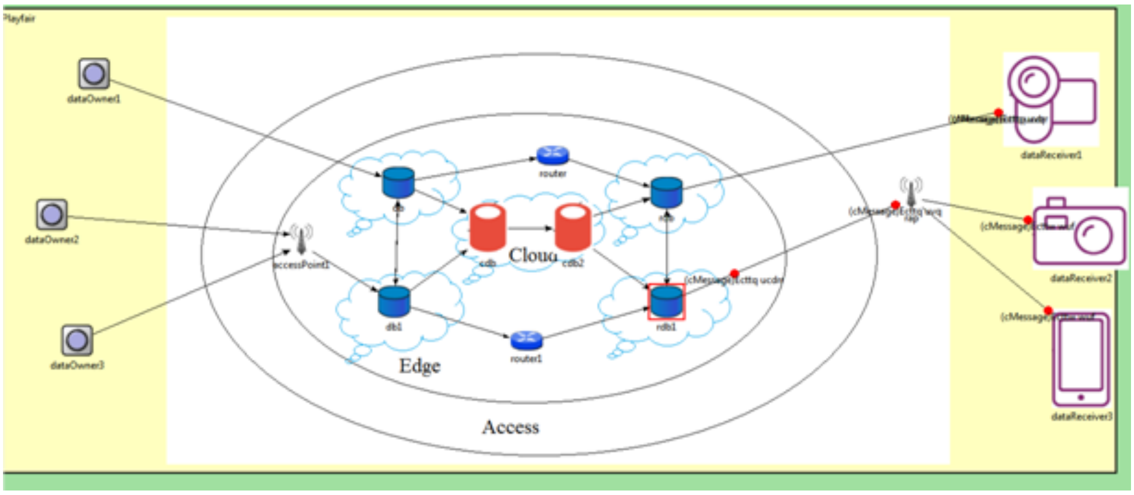


Figure 7:3 The above figure says that the encrypted data is transferred from the database of the cloud to the access point at the receiver side and the receiver side access point to the receiver

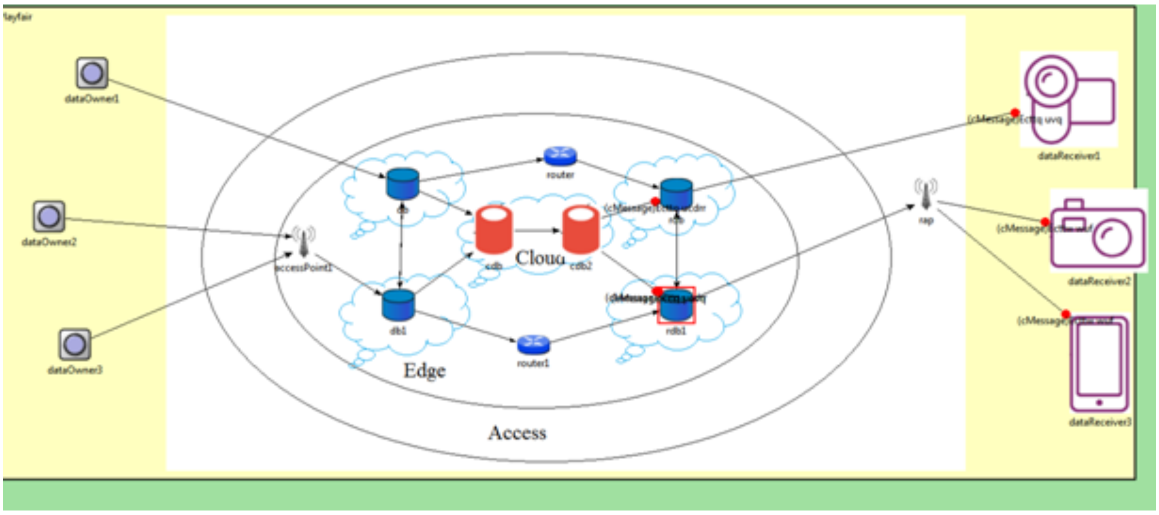


Figure 7:4 The figure illustrates how the data is shared and stored inside the cloud. The encrypted data is shared and it is stored securely in cloud.

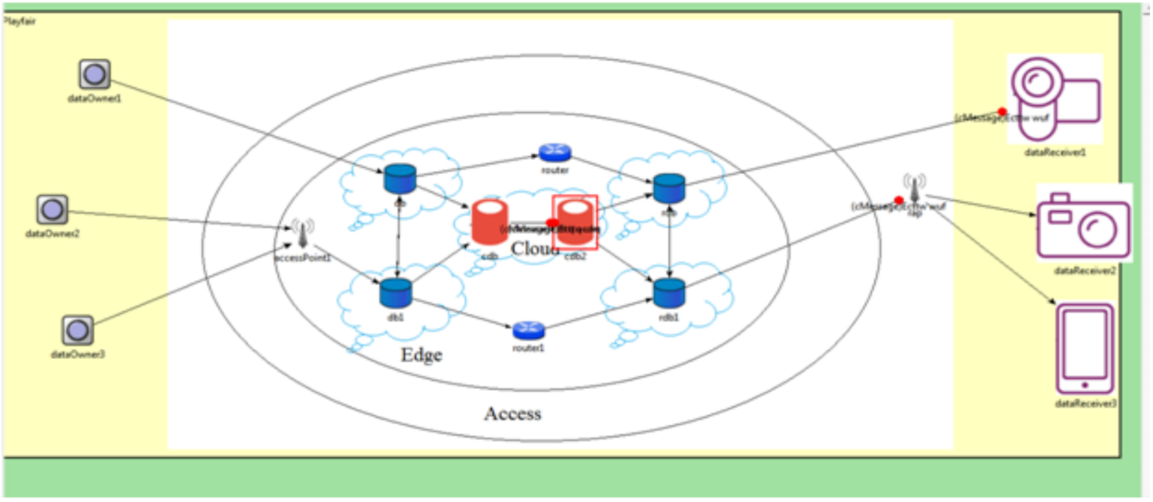


Figure 7:5 Data Transfer from central database of cloud to receiver

The above figure the data is stored in the central database of the cloud. Once the encrypted data is received the data is stored in a central database of the cloud. At the same time if the receiver access the data then the data is transferred between the receiver side with the help of access point.

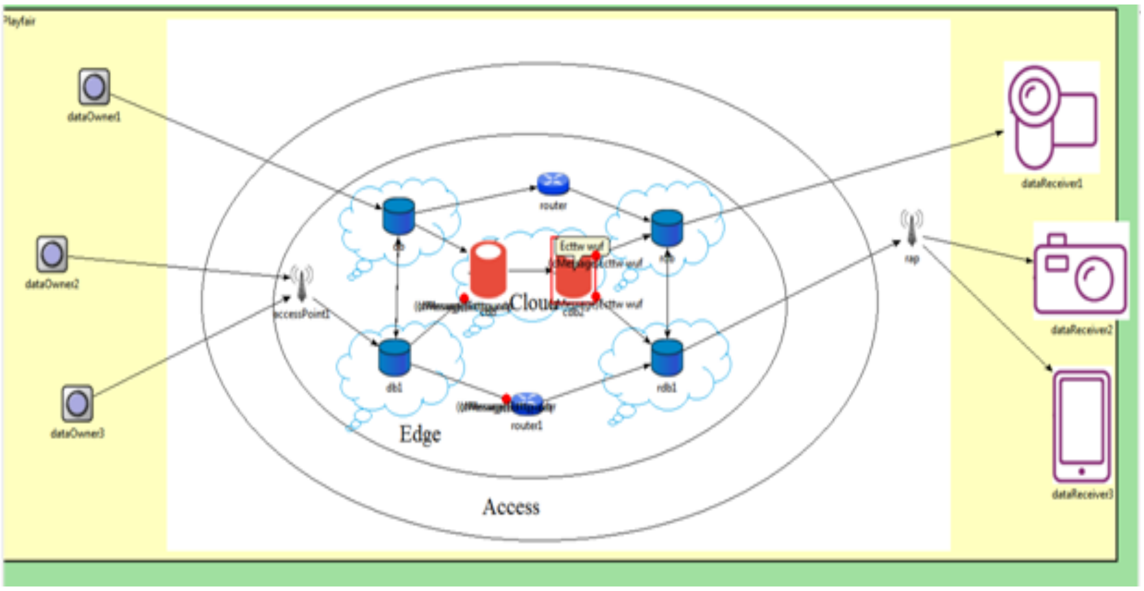


Figure 7:6 The encrypted message is shown as the pop up message before storing in the central database.

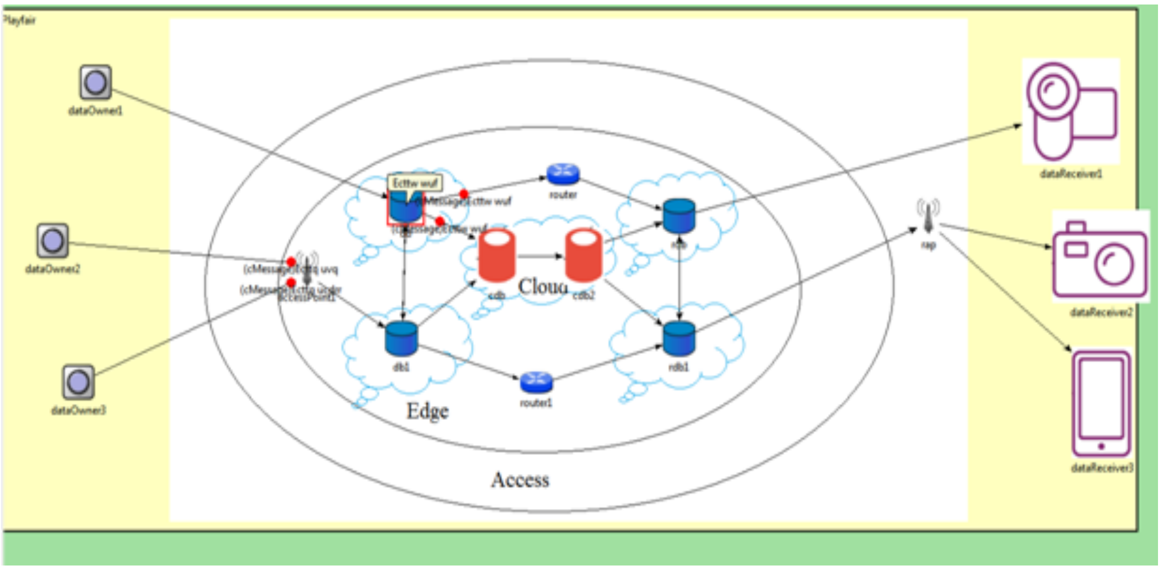


Figure 7:7 Message reached to Sender side & transferred to the cloud

The message is reaching the access point at the sender side and the data is transferred to the cloud. And the cloud stores the data. The encrypted data is shown as the pop up message in the simulation.

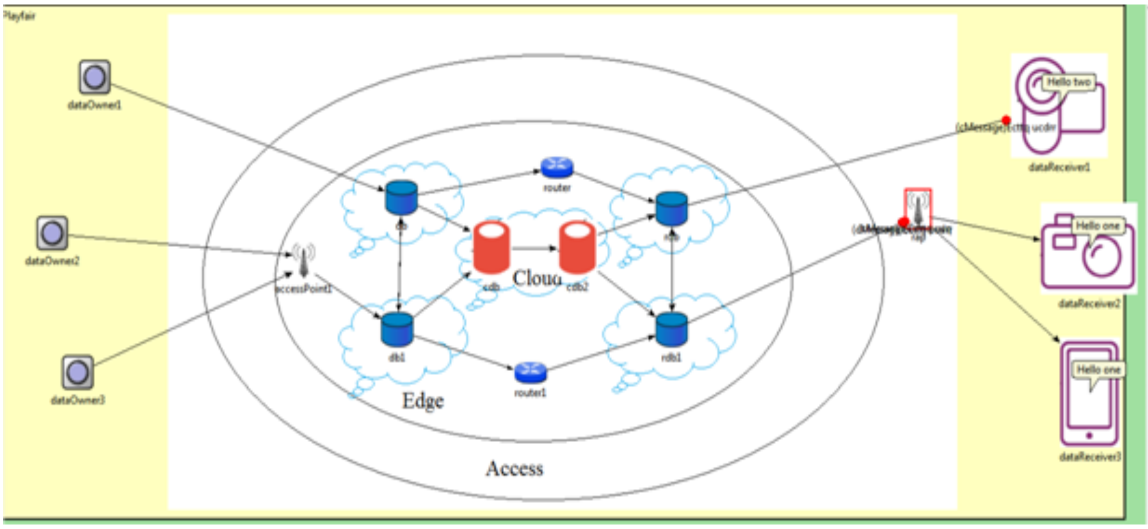


Figure 7:8 Receiver side message decryption

The figure depicts that the data is reaching the receiver side from the receiver side access point and the receiver decrypts the message with the help of the right key. The decrypted data is shown as the pop up message in the simulation

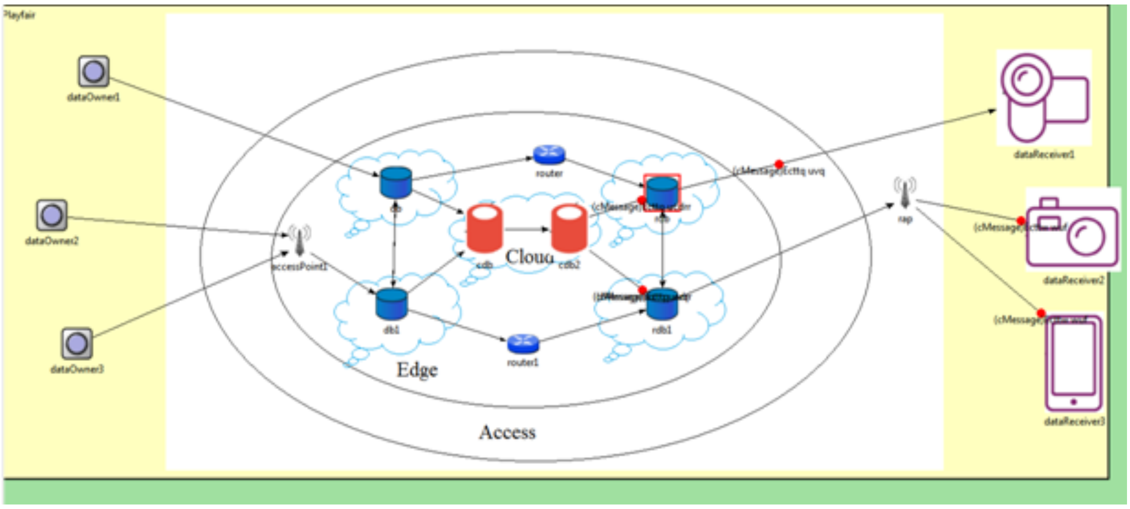


Figure 7:9 Data transfer directly from cloud to receiver

The data is reaching the receiver directly from the database. The receiver1 is directly connected to the cloud database so the receiver can directly receive the message from the database of the cloud.

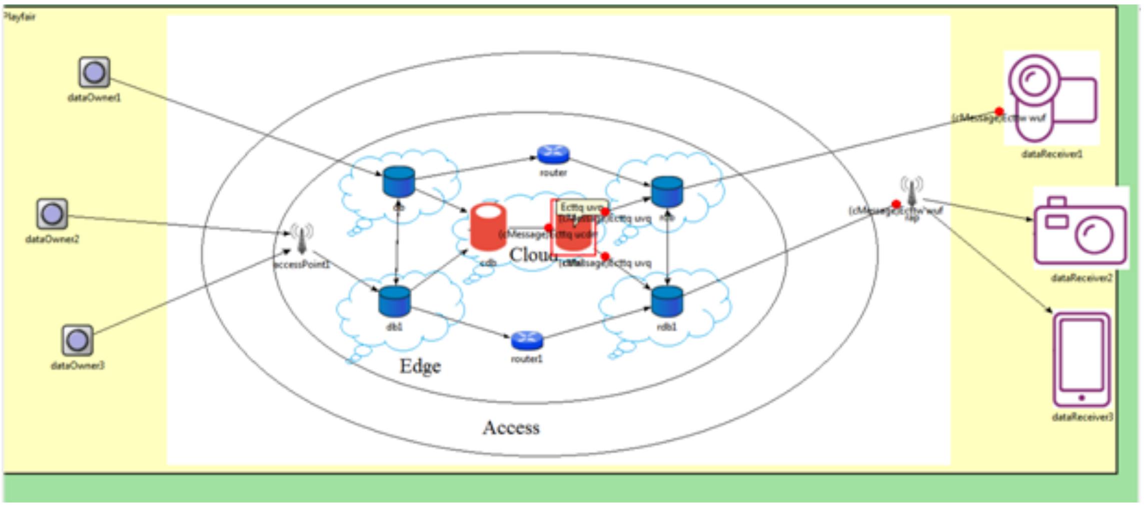


Figure 7:10 The data is stored in the central database of the cloud and the encrypted data is shown as the pop up message in the simulation.

.

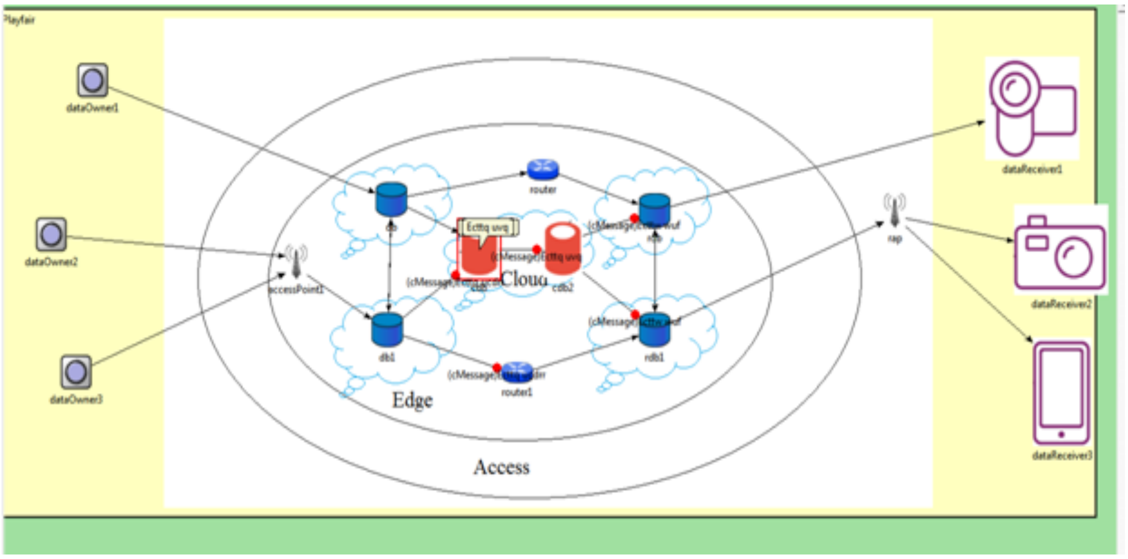


Figure 7:11 The encrypted data is stored in the central database of the cloud. The encrypted data is shown as the pop up message in the simulation

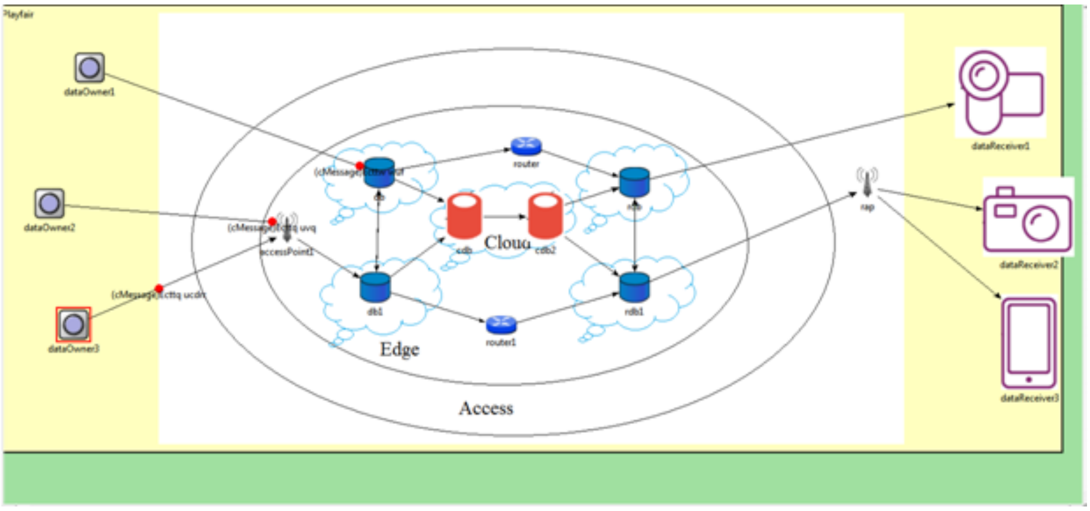


Figure 7:12 The encrypted data is transferred to the cloud through a access point at the sender side.

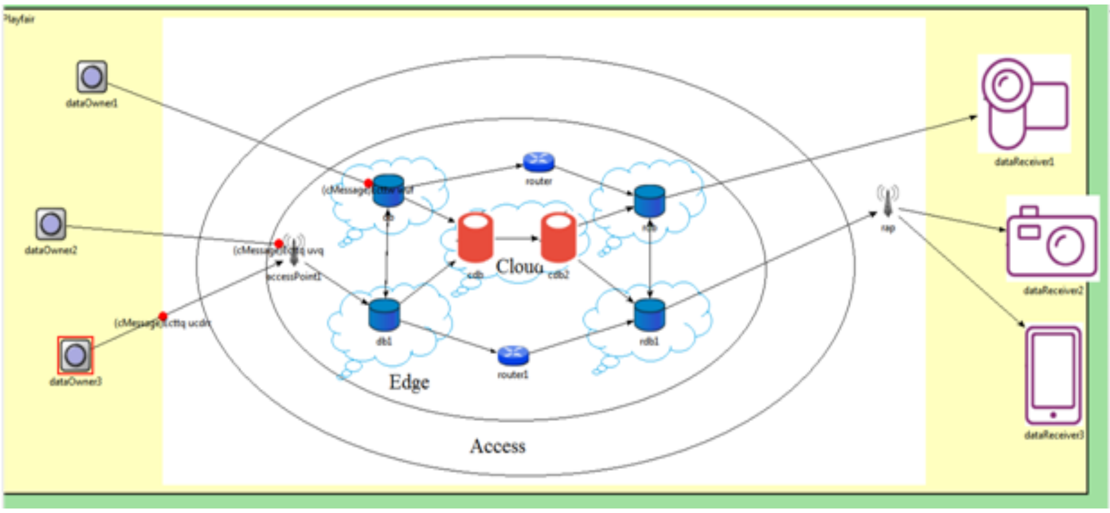


Figure 7:13 The encrypted data is transferred from the owner 2 and owner3 to the cloud through a access point at the sender side.

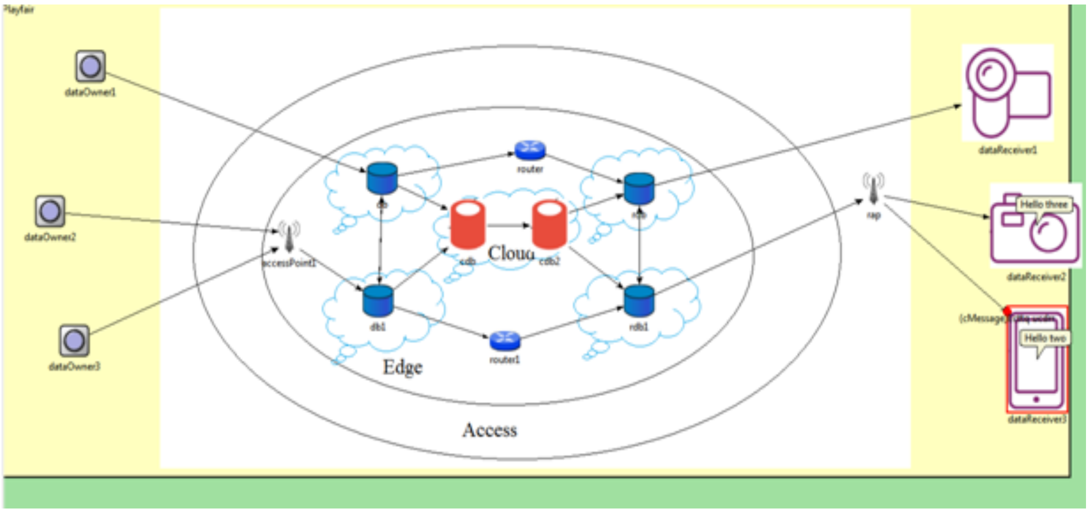


Figure 7:14 The receiver side getting the encrypted message and with the help of key it decrypts the message. The decrypted message is as shown in the figure.

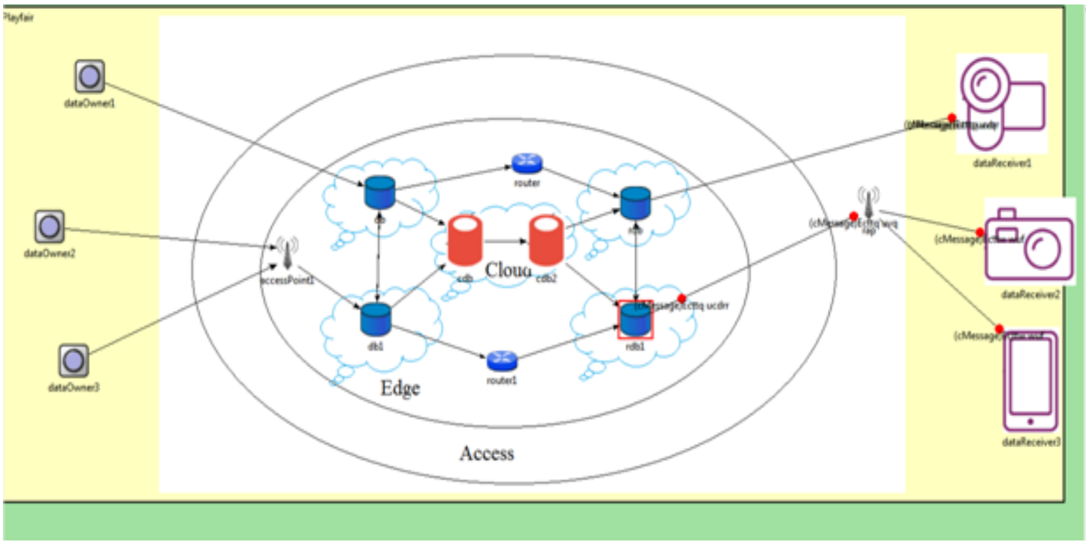


Figure 7:15The encrypted data is transferring from the cloud data base to the receiver side access point.

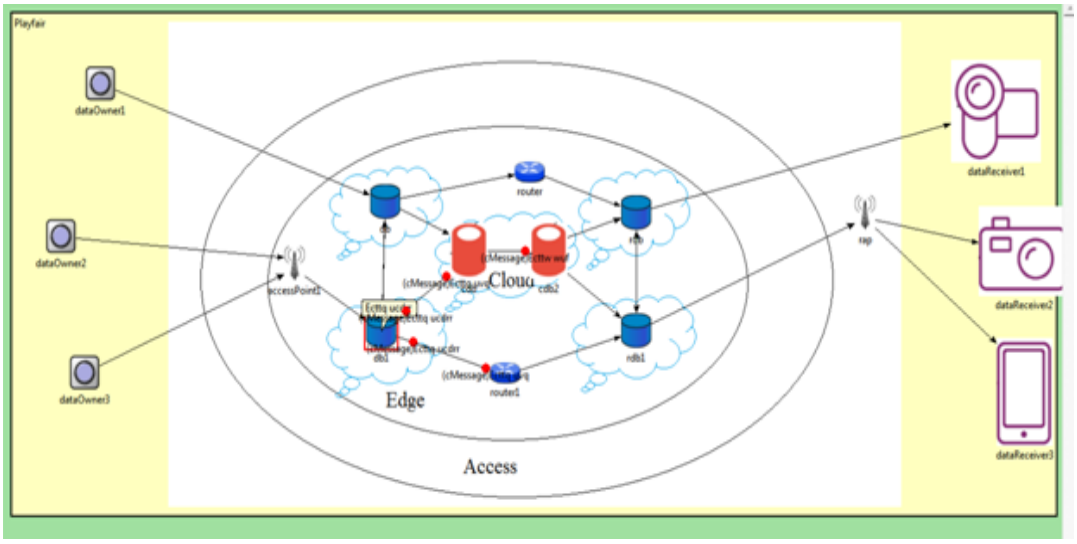


Figure 7:16 The encrypted message is shared and stored securely in the central database of the cloud.

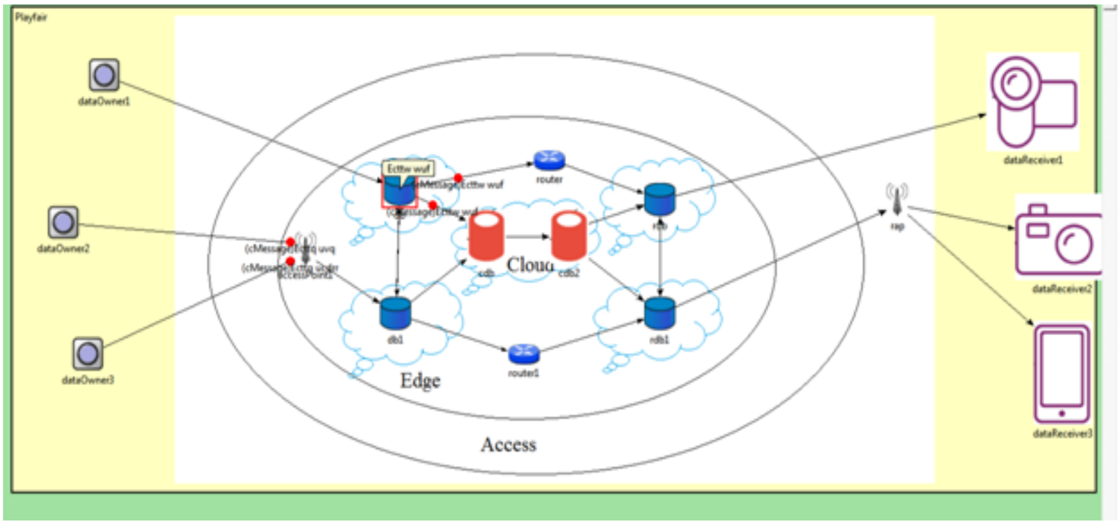


Figure 7:17 The encrypted data is stored in one of the DB in cloud. The encrypted data is as in Pop up.

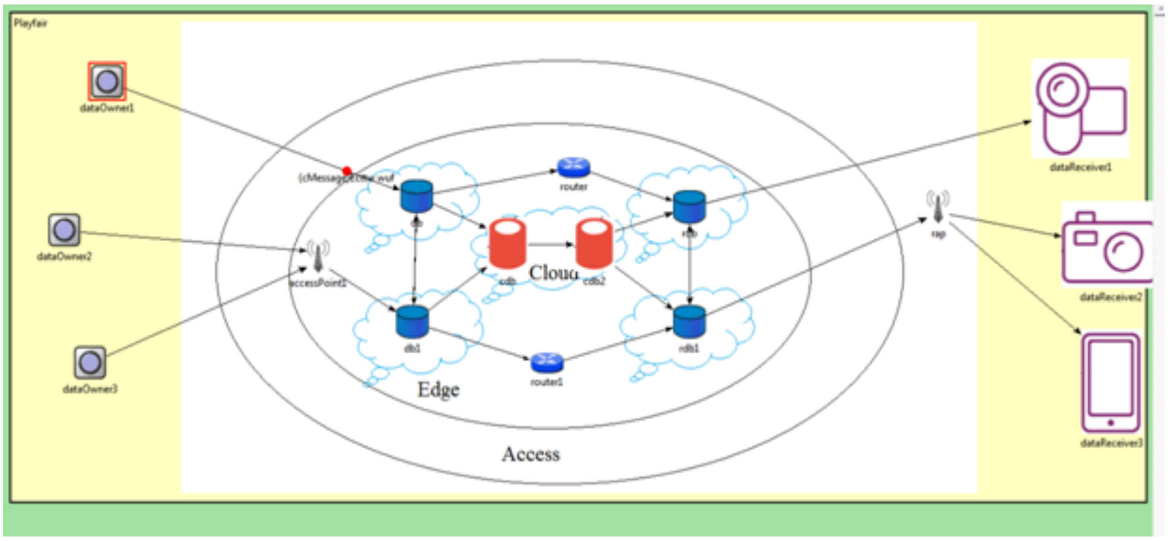


Figure 7:18 Data owner 1 sends data to the cloud once after the encryption is done.

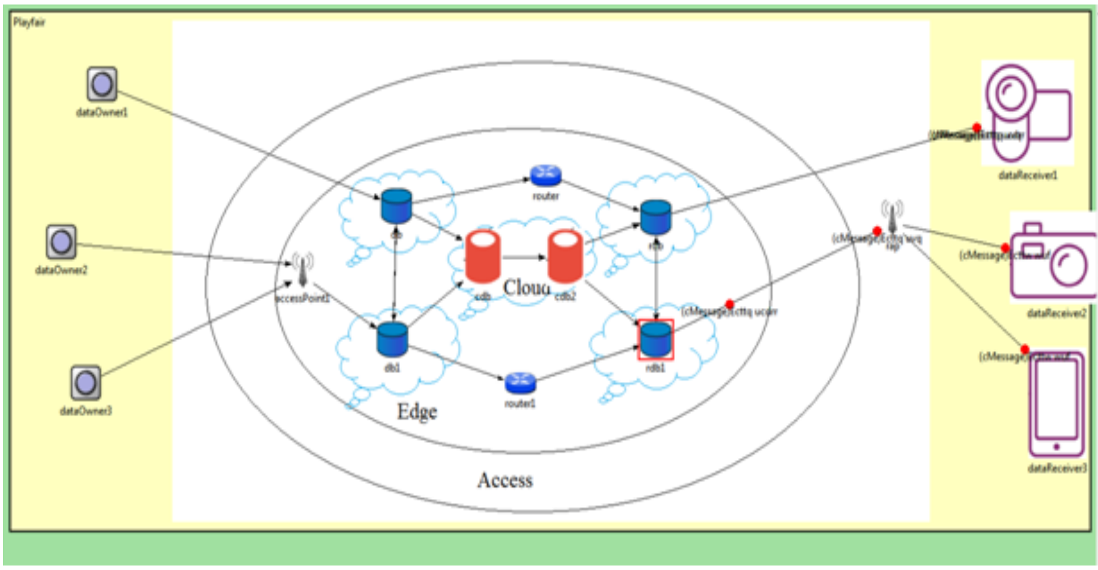


Figure 7:19 The routing data base sends the data to the access point at the receiver side . And the AP sends the data to the corresponding receiver.

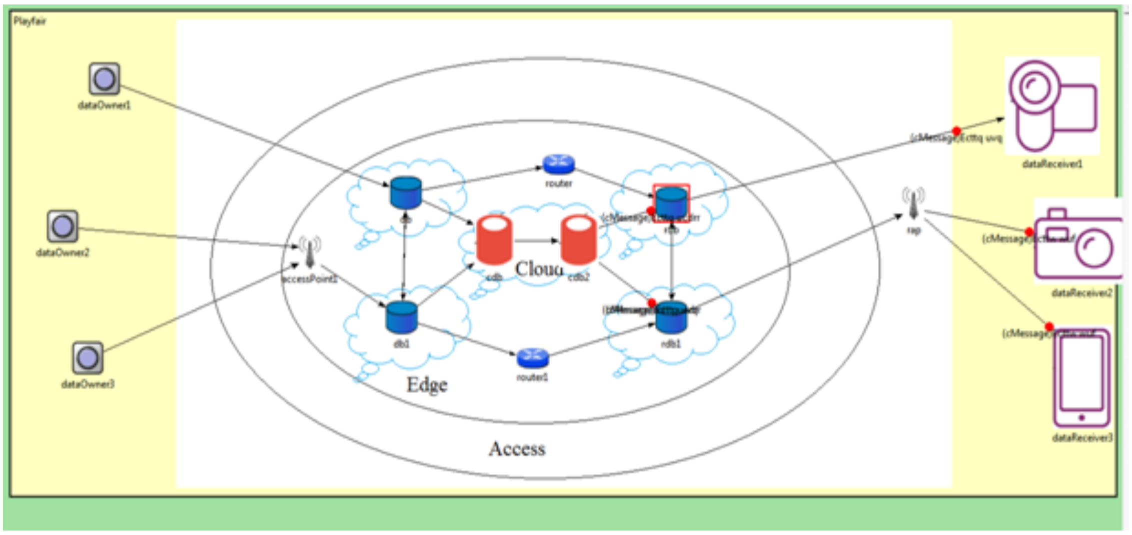


Figure 7:20 The data is transmitted to the routing database from the central database and the data is transmitted to the receiver

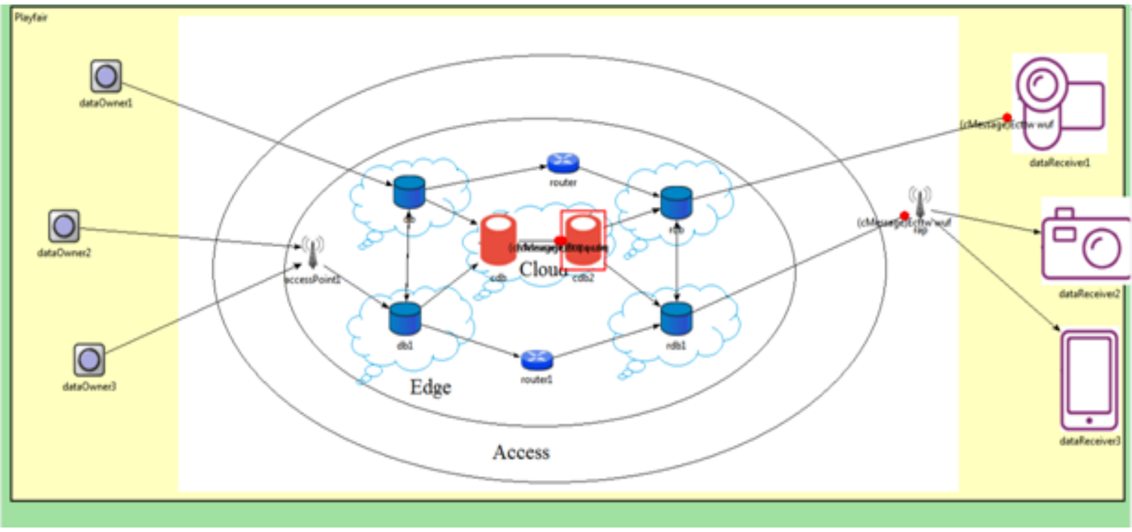


Figure 7:21 The encrypted data is stored in the central database. The data is routed to the receiver1 with the help of RDB.

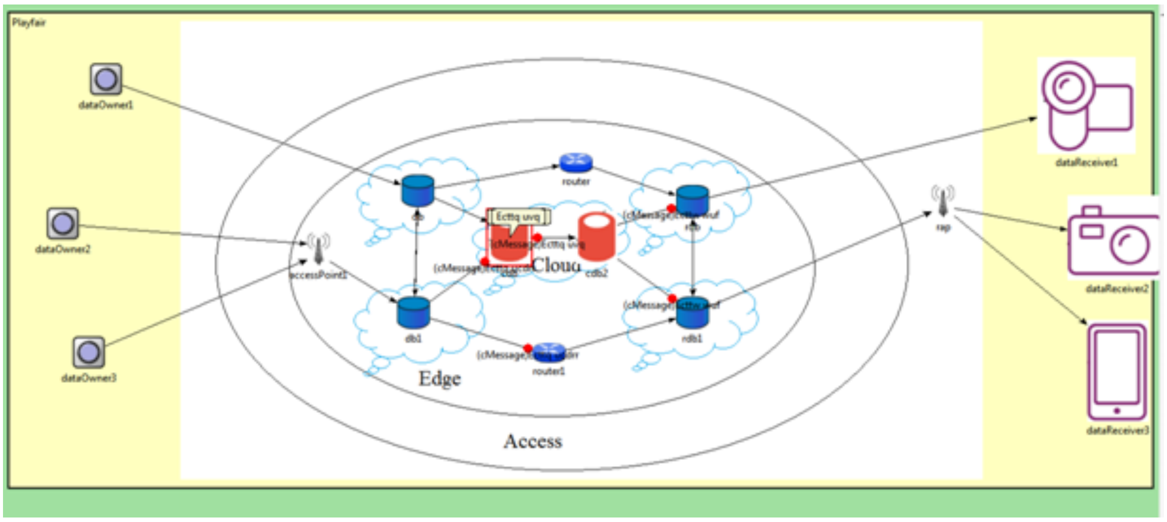


Figure 7:22 The encrypted data is stored inside the cloud and the encrypted message is in the pop up message in the simulation

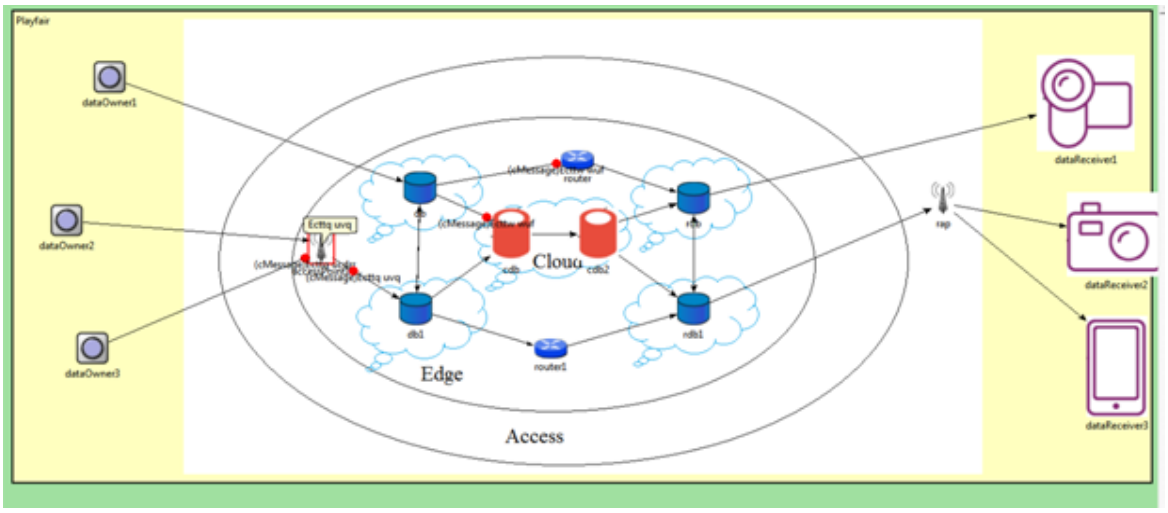


Figure 7:23 The encrypted message is transmitted to the AP from the Owner 2 and Owner 3.

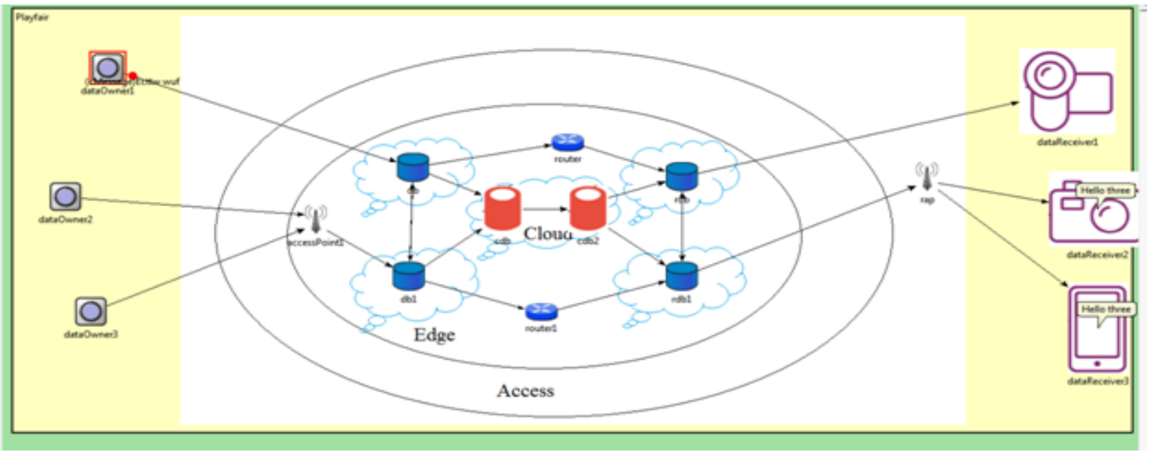


Figure 7:24 The message is transmitted from the data owner1 once after it is encrypted.

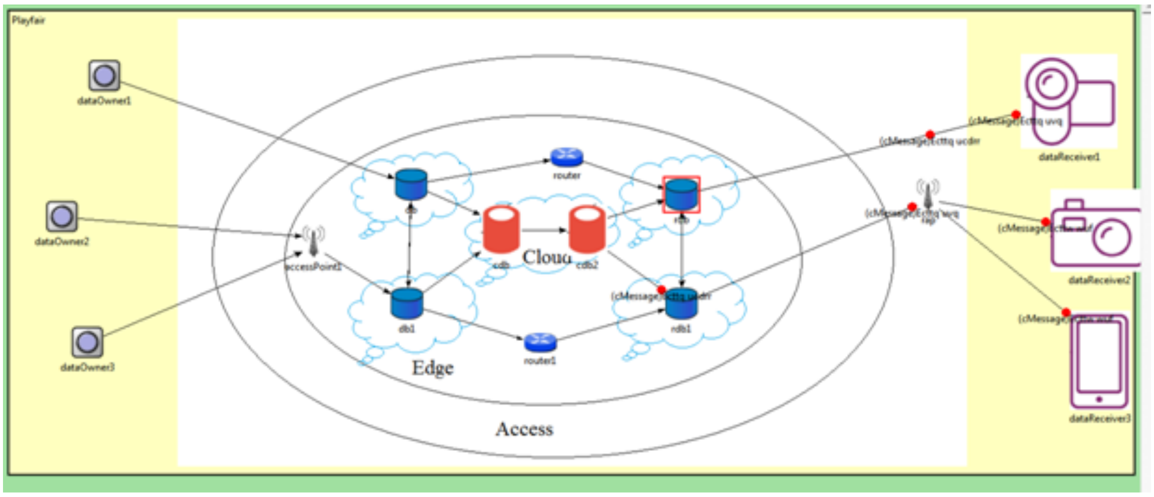


Figure 7:25 The data is transmitted to the AP and the AP transmits the message to the receiver 2 and the receiver 3.

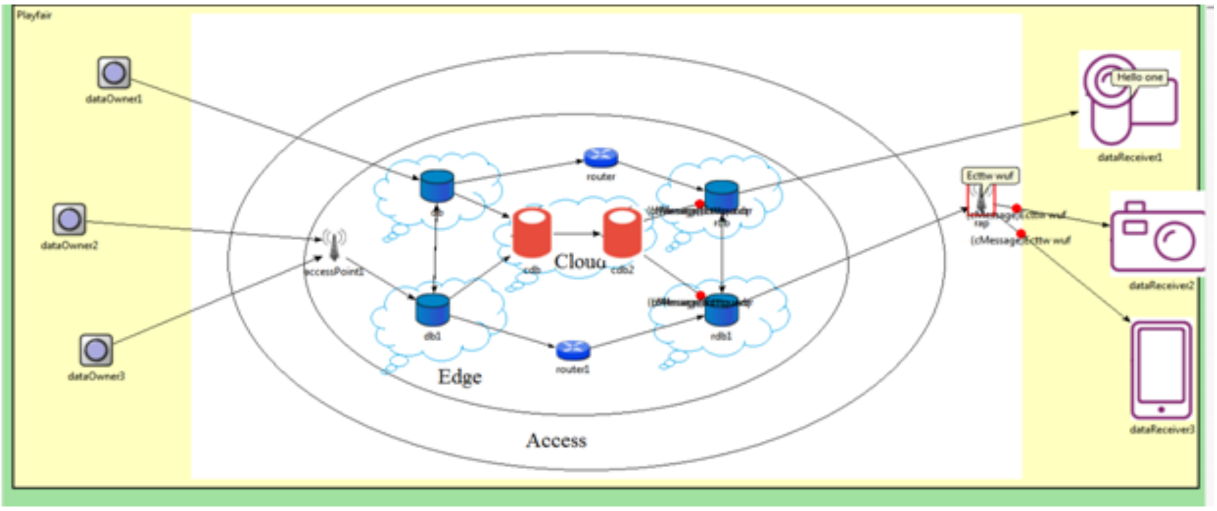


Figure 7:26 The data is transferred to the RDB before it is sent to the AP and the AP transmits the same to receiver correspondingly.

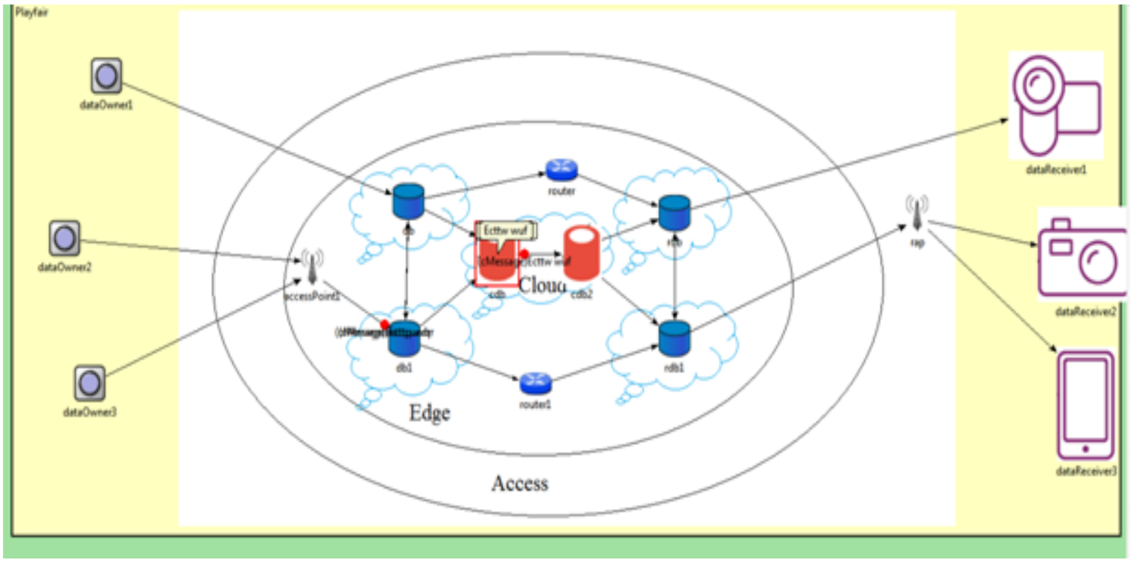


Figure 7:27 The Message is stored in the central database

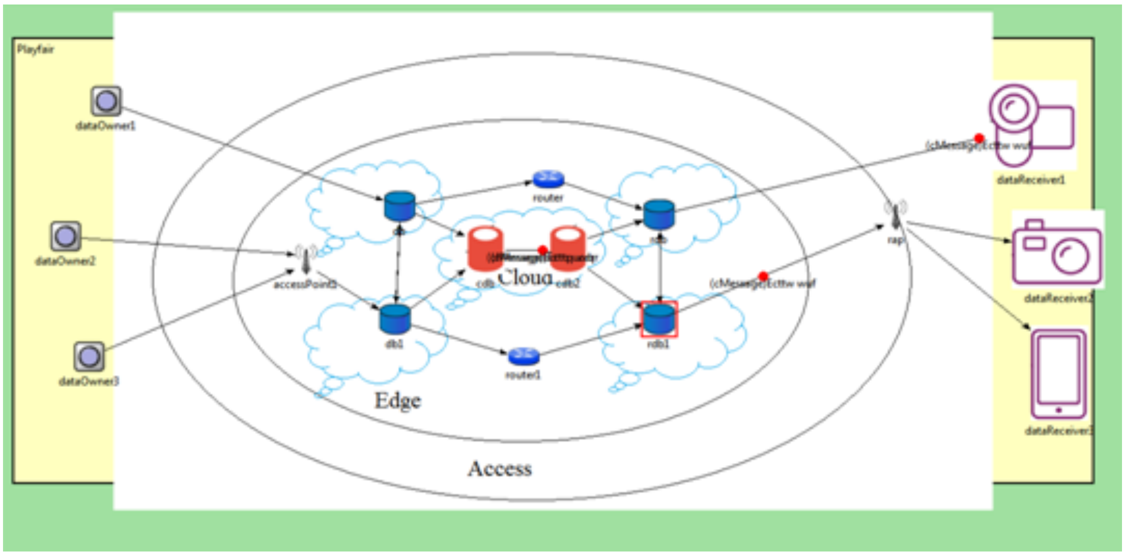


Figure 7:28 The encrypted message is shared and stored in the central db of the cloud and the receiver can access the data from the AP on the receiver side of the cloud.

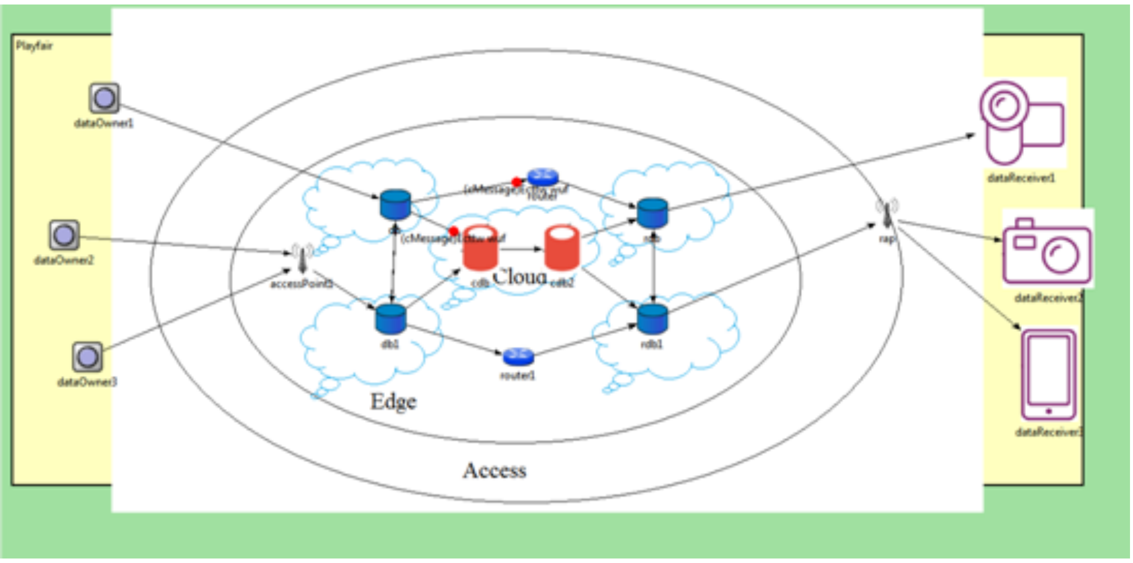


Figure 7:29 The encrypted message is stored in the database of the cloud and the router is used to transmit the message between DB in cloud.

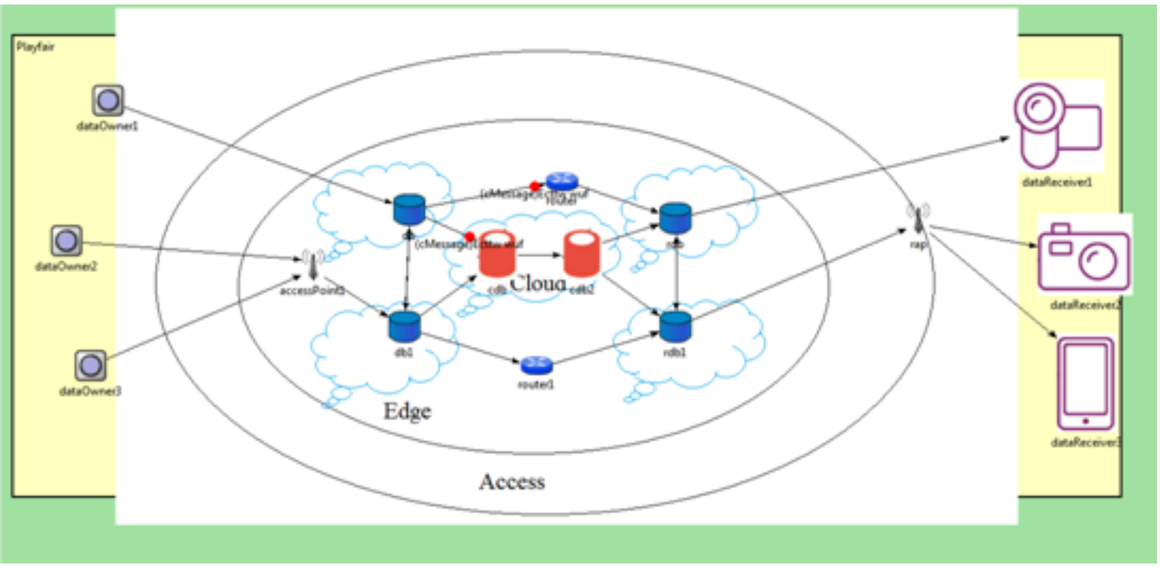


Figure 7:30 The message is routed between the router and the CDB.

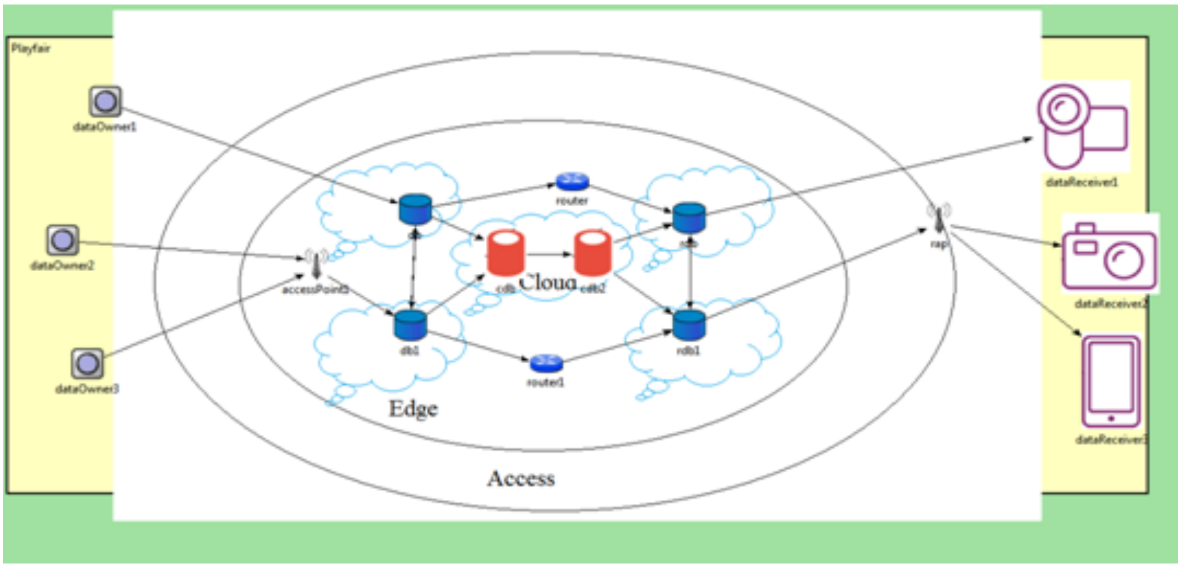


Figure 7:31 The Simulation Scenario

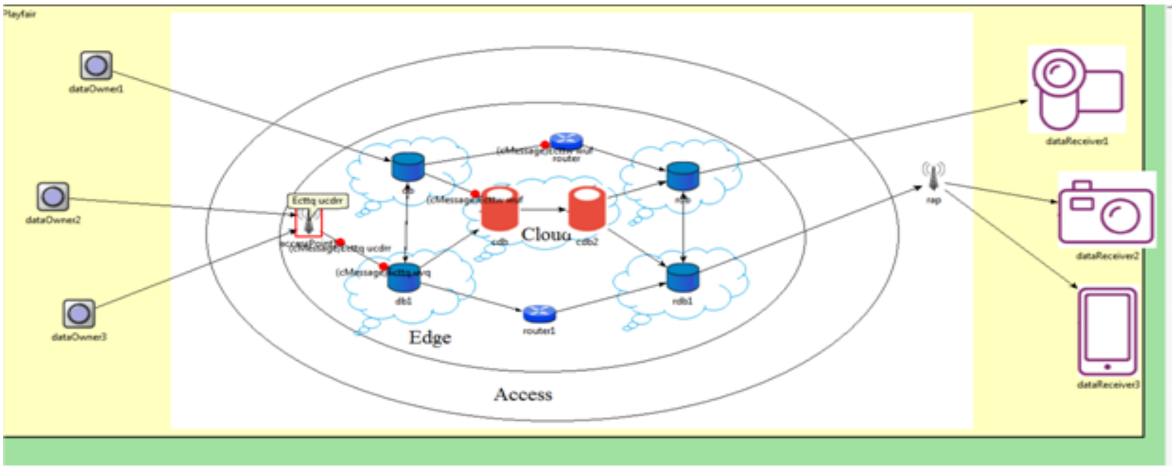


Figure 7:32 The encrypted message is transmitted to AP and the message is transmitted and stored in the DB of cloud.

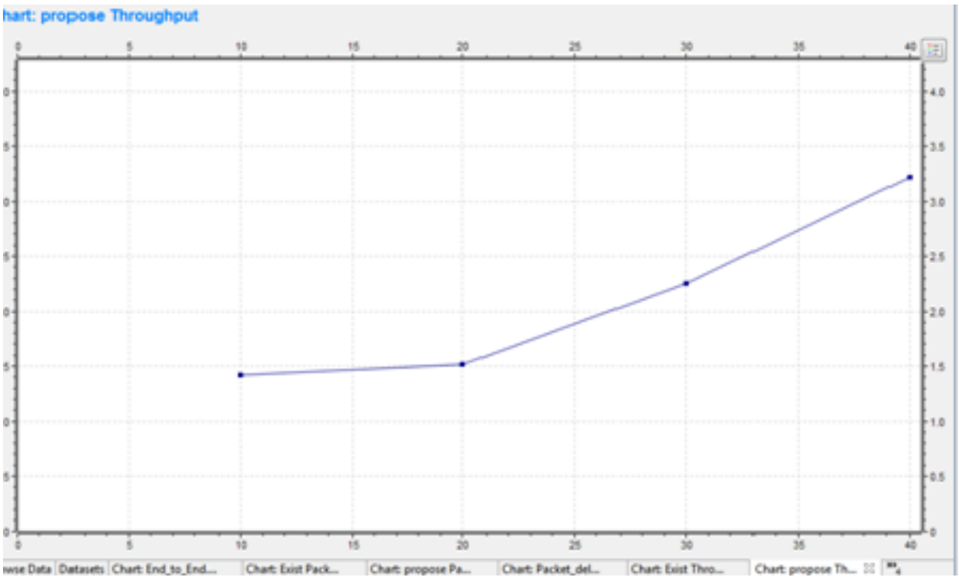


Figure 7:33 The above graph depicts the throughput of the message transmitted between the devices of the cloud (Proposed System).

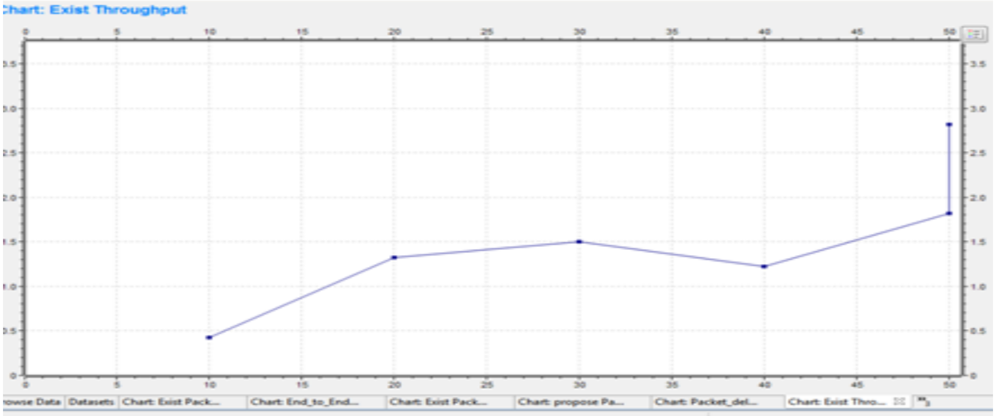


Figure 7:34 : The above graph depicts the throughput of the message transmitted between the devices of the cloud (Existing System).

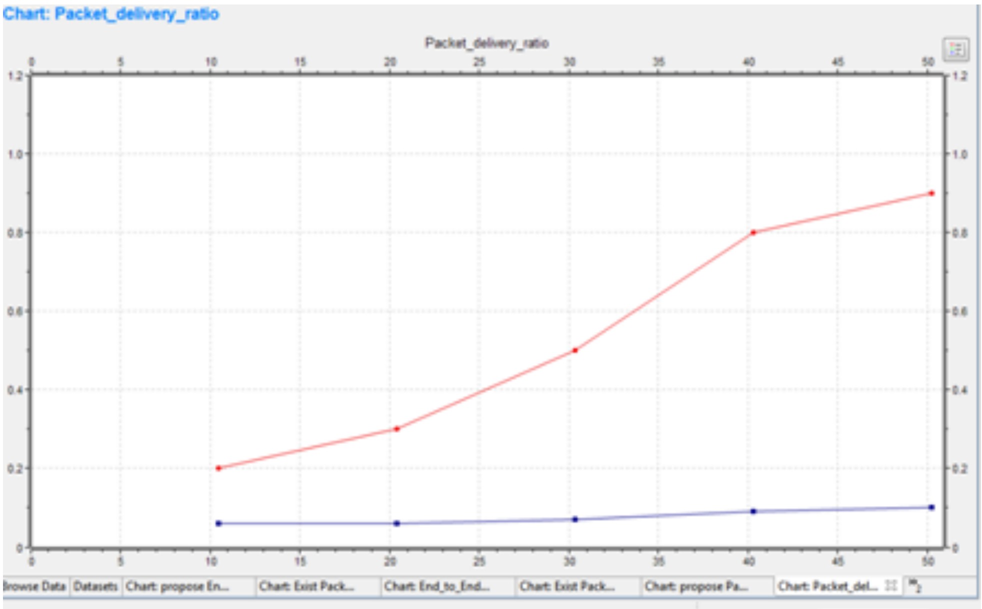


Figure 7:35 The above graph depicts comparison of the Packet Delivery Ratio of the message transmitted between the devices of the cloud (Proposed System & existing System).

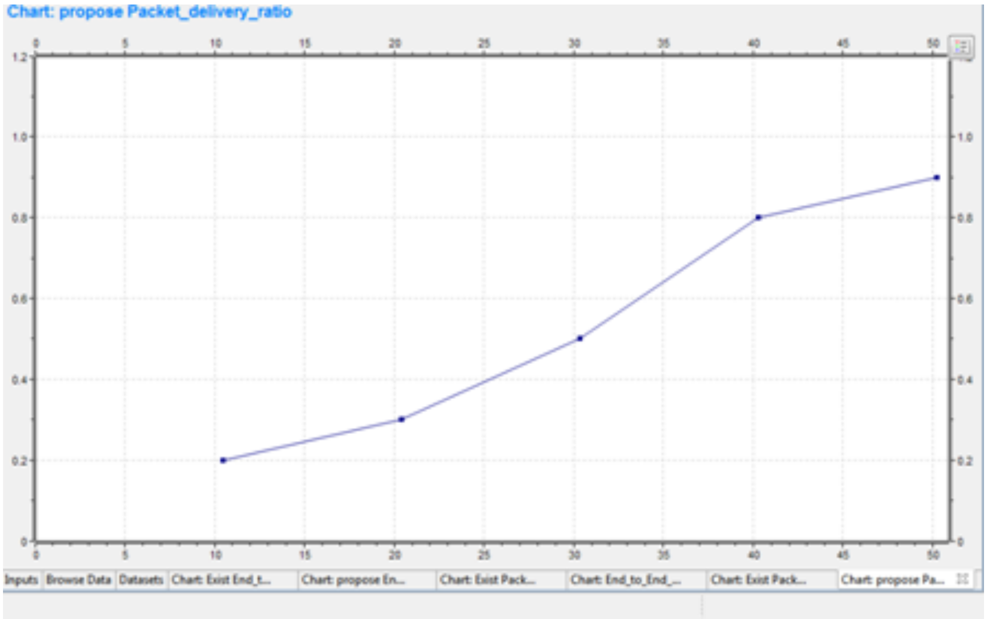


Figure 7:36 The above graph depicts comparison of the Packet Delivery Ratio of the message transmitted between the devices of the cloud (Proposed System).

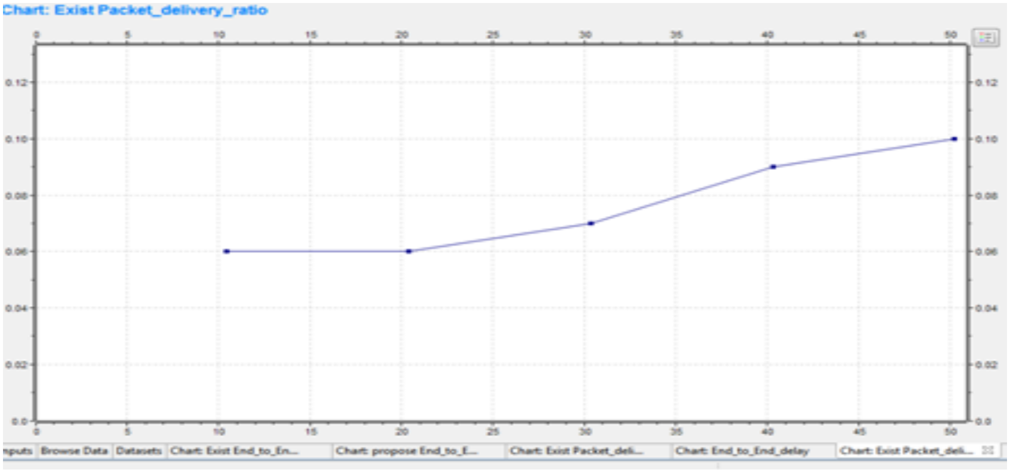


Figure 7:37 The above graph depicts comparison of the Packet Delivery Ratio of the message transmitted between the devices of the cloud (existing System).

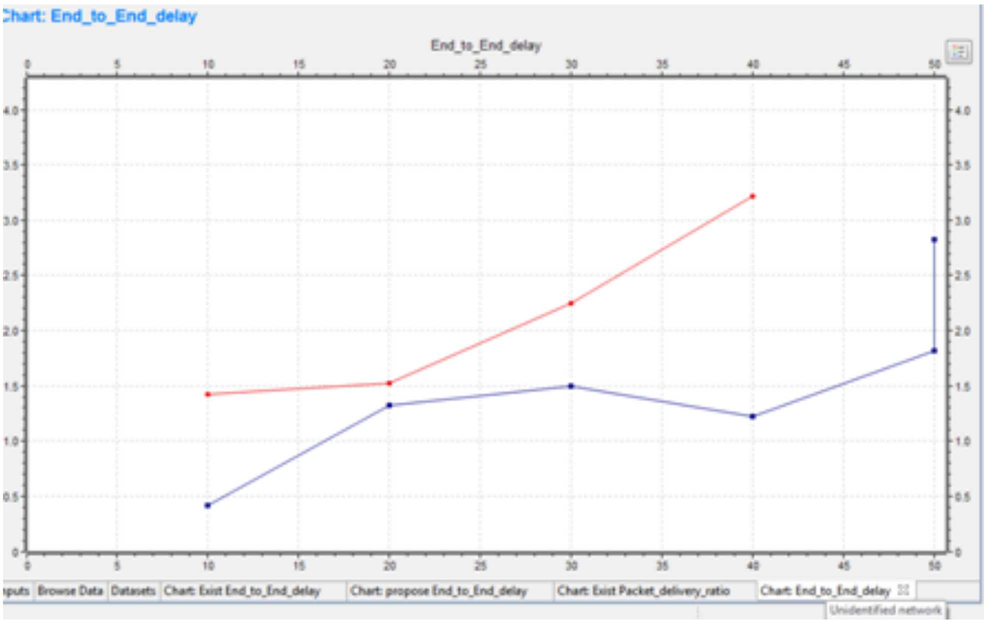


Figure 7:38 The above graph depicts comparison of End to end delay of the message transmitted between the devices of the cloud (Proposed System & existing System).

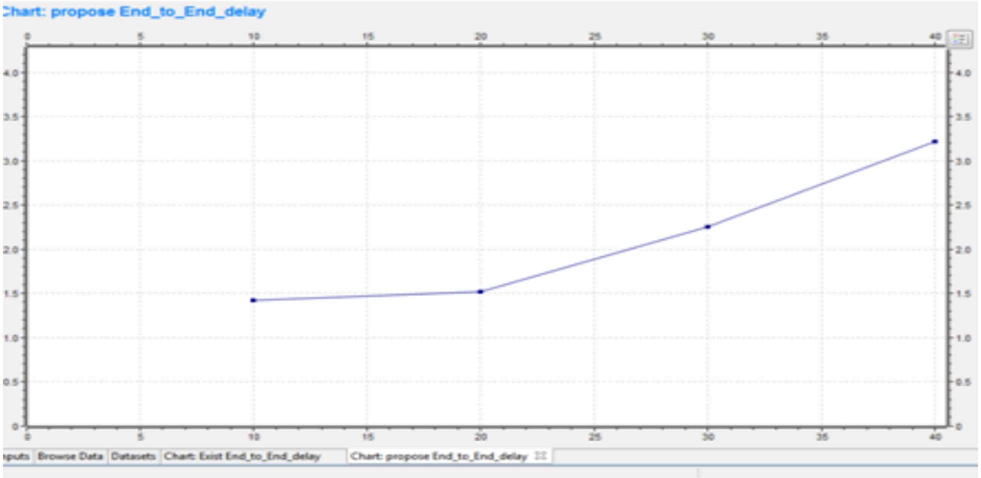


Figure 7:39 The above graph depicts comparison of End to end delay of the message transmitted between the devices of the cloud (Proposed System).

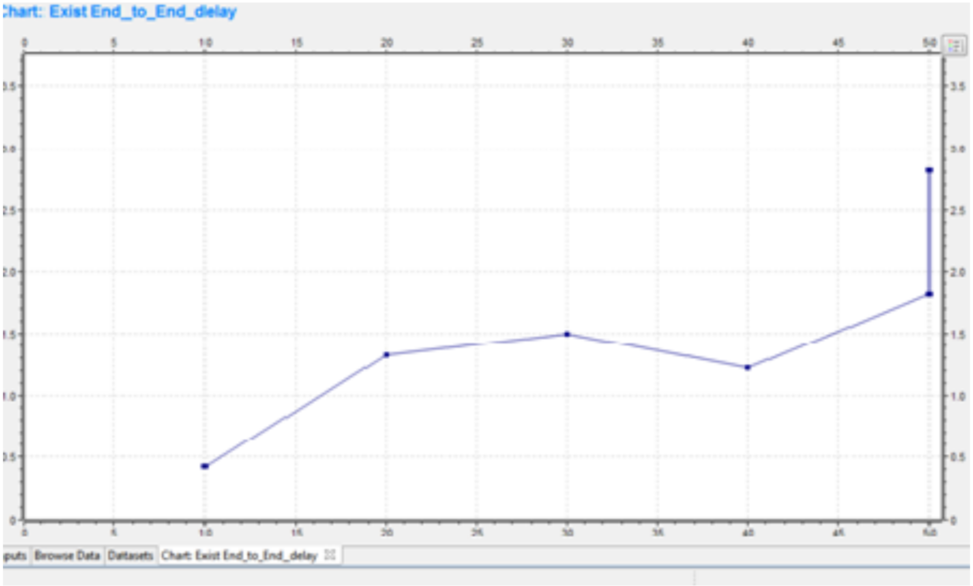


Figure 7:40 The above graph depicts comparison of End to end delay of the message transmitted between the devices of the cloud (Proposed System & existing System

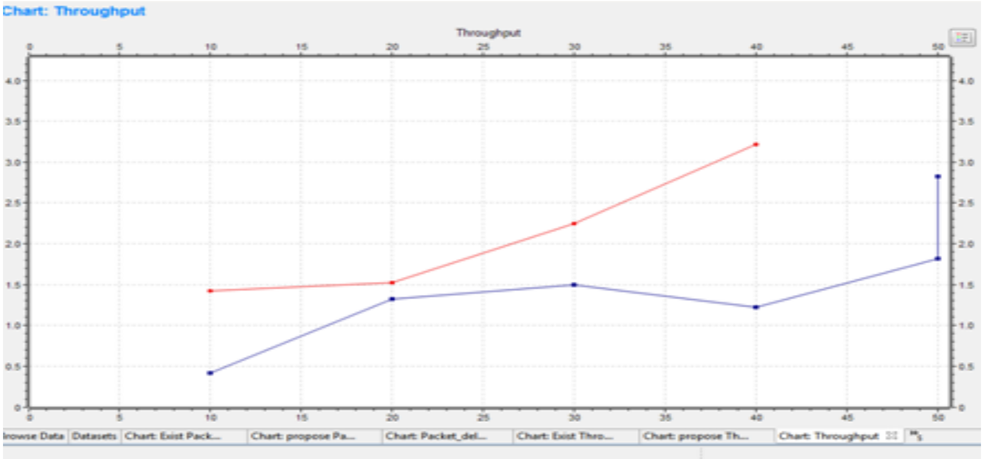


Figure 7:41 The above graph depicts comparison of throughput of the message transmitted between the devices of the cloud (Proposed System & existing System).

Chapter 8

8 Chapter 8 : Conclusion & Future Scope

Any developing organization need to store the data that need to reduce the storage cost is mandatory. So that the data helps them in many decision making systems. So, only if the cloud ensures the security then only the organization will come forward to store the data in cloud. So the cloud providers need to develop a trust between the organizations. A numerous algorithm are provided for the protection of data and to provide highest security in cloud. In this paper we have proposed a new technology that provides high security from the security attack. In this paper we have proposed a advanced algorithm called advanced wheat stone algorithm. The data sensed from the devices is encrypted and stored in cloud and the key is shared with the receiver so that the receiver can decrypt the sensed data from the cloud. The third party cannot read the data from the cloud. The proposed system is safer when compared to the existing system. Implemented as per the objectives in the chapter-1 using Omnet ++ simulation tool to simulate the entire scenario. I have obtained better results comparatively.

Future Scope:

Mobile cloud computing promises several benefits such as extra battery life and storage, scalability, and reliability. However, there are still challenges that must be addressed in order to enable the ubiquitous deployment and adoption of mobile cloud computing. Some of these challenges include security, privacy and trust, bandwidth and data transfer, data management and synchronization, energy efficiency, and heterogeneity. May be proposed thorough overview of mobile cloud computing and differentiate it from traditional cloud computing. Also future requirement is a generic architecture that evaluates so many recently proposed mobile cloud computing research architectures. This is achieved by utilizing a set of assessment criteria. Finally, the future research challenges that require further attention.

Part II - Publications of the Author

I Paper Publications

Scopus & Elsevier Scopus Papers

Total : 10

1. Blockchain Cyber Security Vulnerabilities and Potential Counter measures, International Journal of Innovative Technology and Exploring Engineering (IJITEE) Dr.K.Sai Manoj Dr.P.S.Aithal ISSN: 2278-3075,Volume-9, Issue-5, March2020 http://www.ijitee.org/wp-content/uploads/papers/v9i5/E2170039520.pdf
2. Data Mining and Machine Learning Techniques for Cyber Security Intrusion Detection International Journal of Engineering and Advanced Technology (IJEAT) Dr.K.Sai Manoj Dr.P.S.Aithal ISSN: 2249 - 8958, Volume-9 Issue-3, February, 2020 https://www.ijeat.org/download/volume-9-issue-3/
3. Adaptive Street Light Monitoring Using Internet of Things, International Journal of Advanced Science and Technology, Dr.K.Sai Manoj, Volume-29 Bo:7s(Special Issue), June 2020. http://sersc.org/journals/index.php/IJAST/article/view/25699
4. A Novelty on Mobile Devices Fast Authentication and Key Agreement, International Journal of Psychosocial Rehabilitation (ISSN: 1475-7192), Dr.K.Sai Manoj, Volume-24, Issue -8, February 2020. https://www.psychosocial.com/article/PR281261/27994/
5. Design and Development of Various Cloud Computing Architectures Improving the Security International Journal of Innovative Technology and Exploring Engineering (IJITEE)Dr.K.Sai Manoj ISSN: 2278-3075, Volume-8 Issue-12S2, October 2019)
6. Research on the Security Policies for Cloud Computing International Journal of Innovative Technology and Exploring Engineering (IJITEE) Dr.K.Sai Manoj ISSN: 2278-3075, Volume-8 Issue-12S2, October 2019http://www.ijitee.org/wp-content/uploads/papers/v8i12S2/L107610812S219.pdf
7. Conceptual based on the Data Mining Techniques for the Prediction of Hydration Assessment, Breath Analysis and Heart Disease International

Journal of Innovative Technology and Exploring Engineering (IJITEE) Dr.K.Sai Manoj ISSN: 2278-3075, Volume-8 Issue-12S2, October 2019 http://www.ijitee.org/wp-content/uploads/papers/v8i12S2/L107510812S219.pdf

8. Conceptual oriented study on the cloud computing architecture for the full-security, Dr.K.Sai Manoj International Journal of Engineering & Technology, Science Publishing Corporation (First Author) (SPC) https://www.sciencepubco.com/index.php/ijet/article/view/11654

9. Cloud security: risk factors and security issues in current trends Dr.K.SaiManoj International Journal of Engineering & Technology, Science Publishing Corporation October 2019 (Scopus) (Single Author) https://www.sciencepubco.com/index.php/ijet/issue/view/495

10. Risk Factors And Security Issues In Various Cloud Storage Operations Dr.K.Sai Manoj Volume-8 Issue-12, October 2019, ISSN: 2278-3075 (Online) Published By: Blue Eyes Intelligence Engineering & Sciences Publication (First Author) (Elsevier Scopus)

Thomson Reuters & UGC Approved Papers

Total: 10

1. CHALLENGING ISSUES RELATED TO SOME SPECIFIC IMPORTANT PROBLEMS IN THE CLOUD PLATFORM by Dr.K.Sai Manoj published in the merit list by International Journal of Computer Engineering and Applications Volume XIII, Issue VIII August 2019. (UGC Approved Journal with Thomson researcher id) (Single author)

2. Conceptual Oriented Analysis On The Industrial Standard Cyber Security by Dr.K.Sai Manoj published in International Journal of Computer Science Trends and Technology (IJCST) – Volume 7 Issue 4, Jul - Aug 2019 (Single author) http://www.ijcstjournal.org/volume-7/issue-4/IJCST-V7I4P3.pdf

3. CONCEPTUAL ORIENTED ANALYSIS ON THE IMPACT ON THE CLOUD SECURITY ON THE CYBER ATTACKS by Dr.K.Sai manoj selected in the merit list by Journal of Analysis and Computation (JAC) (An

International Peer Reviewed Journal), www.ijaconline.com, ISSN 0973-2861 Volume XII, Issue I, May 2019 (First Author) http://www.ijaconline.com/conceptual-oriented-analysis-impact-cloud-security-cyber-attacks/

4. INVESTIGATIONS ON THE CLOUD DATA STORAGE SECURITY BASED USING DIFFIE HELLMAN ALGORITHM by Dr.K.Sai Manoj selected in the merit list by International Journal of Computer Engineering and Applications, Volume XIII, Issue VI, JUNE. 19, www.ijcea.com ISSN 2321-3469 (First Author) http://www.ijcea.com/investigations-cloud-data-storage-security-based-using-diffie-hellman-algorithm/
5. Analysis of the Technique for the Improvement of the Data Confidentiality in the Cloud Computing Environment by Dr.K.Sai Manoj Published in international Journal of Computer Science Trends and Technology (IJCST) – Volume 7 Issue 4, Jul - Aug 2019 (First Author) http://www.ijcstjournal.org/volume-7/issue-4/IJCST-V7I4P5.pdf
6. Conceptual oriented analysis on the modern tools and techniques to Enrich Security Vulnerabilities in Ethical Hacking Dr.K.Sai Manoj International Journal of Computer Science Trends and Technology (IJCST) in May-June 2019, Volume Number 7 Issue3 with ISSN: 2347-8578 & ISO 3297:2007.This Journal has Thomson Reuters ResearcherID: M-3066-2016. (First Author) http://www.ijcstjournal.org/volume-7/issue-3/IJCST-V7I3P25.pdf
7. Investigation on the Cloud Computing in terms of the current trends and also to meetthe important challenges with security for the improvement of the Health care services Dr.K.Sai Manoj IJCEA Feb. 2019, with Thomson Reuters Research Id: P1671-2016. Also It is UGC approved Journal. For this article author Dr.K.Sai Manoj research article in the merit list from the Reviewers and Editorial Team. (First Author) http://www.ijcea.com/investigation-cloud-computing-terms-current-trends-also-meet-important-challenges-security-improvement-health-care-services/
8. Investigation on the security aspects of the cloud computing using symmetric and asymmetric algorithms , Dr.K.Sai Manoj International Journal of Computer Engineering and Applications, Volume XIII, Issue I, January. 19, www.ijcea.com ISSN 2321-3469 with Thomson Reuters Research Id: P1671-

2016. Also It is UGC approved Journal. For this article author Dr.K.Sai Manoj received appreciation certificate in the merit list from the Editor. (**First Author)** http://www.ijcea.com/investigation-security-aspects-cloud-computing-using-symmetric-asymmetric-algorithms/

9. Investigation on the Attribute Based Encryption for Secure Data Access in Cloud, Dr.K.Sai Manoj International Journal of Computer Science Trends and Technology (IJCST) with Thomson Reuters Researcher ID: M-3066-2016 – Volume 6 Issue 6, Nov-Dec 2018. ISSN: 2347-8578 (First Author) https://www.scribd.com/document/393639933/IJCST-V6I6P13-Dr-K-SAI-MANOJ-Ms-K-Mrudula-Mrs-K-Maanasa-K-Phani-Srinivas
10. INVESTIGATION ON THE DATA SECURITY IN CLOUD COMPUTING USING BIOMETRICS International journal of current advanced research UGC approved and also Thomson Reuters journal with researcher id and END NOTE ISSN: O: 2319-6475, ISSN: P: 2319-65,Impact factor:6.614, Volume 7;Issue 12(B);December 2018;Page No.16473-16475.(First Author) http://journalijcar.org/issues/investigation-data-security-cloud-computing-using-biometrics

Thomson Reuters Papers

Total: 4

1. Conceptual Oriented Analysis on the Security based on the SaaS Cloud Computing Architecture for the Cyber Security Issues by Dr.K.Sai Manoj published in International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177 Volume 7 Issue VII, July 2019 (**First Author)** https://www.ijraset.com/fileserve.php?FID=24254
2. A Study on identifying defects and solutions of search engines, Dr.K.Sai Manoj, Global Journal of Engineering Science and Research Management – January 2018 (Second Author)
3. INVESTIGATION ON THE ON THE CLOUD COMPUTING SECURITY USING PET AND

REMOTE ATTESTATION IN CLOUD ARCHITECTURES by Dr.K.Sai Manoj published in International Journal of Current Advanced Research Volume 8; Issue 10 (D); October 2019 http://dx.doi.org/10.24327/ijcar.2019 Impact Factor: 6.614 ISSN: O: 2319-6475, ISSN: P: 2319-6505 ; October 2019http://journalijcar.org/issues/investigation-cloud-computing-security-using-pet-and-remote-attestation-cloud-architectures

4. Research on Security and Vulnerabilities of Blockchain Systems by Dr.K.Sai Manoj published in International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177 Volume 8 Issue I, Jan 2020 (Single Author)https://www.ijraset.com/fileserve.php?FID=26233

UGC Approved Journal Papers

Total: 3

1. Investigation on the Data Protection in the Cloud using Predicate Based Encryption International Journal of Computer Science and Information Technology Research UGC approved with ISSN 2348-120X (online) Vol. 6, Issue 4, pp: (61-65), Month: October - December 2018.(First Author) http://www.researchpublish.com/journal/IJCSITR/Issue-4-October-2018-December-2018/0
2. Content Filtering and cloud based intrusion detection system, Dr.K.Sai Manoj, Global Journal of Engineering Science and Research Management – January 2018 (First Author – Thomson Reuters)
3. A Survey on Protection of Multimedia Content in Cloud Computing, Dr. K.Sai Manoj, Mrudula Kudaravalli, International Journal of Computer Science and Mobile Computing - Vol.6 Issue.11, November- 2017, pg. 7-11 (First Author) http://ijcsmc.com/docs/papers/November2017/V6I11201705.pdf

Google Scholar related Research Papers

Total: 11

1. UNCRACKABLE CIPHER DYNAMIC DOUBLE ENCRYPTION STANDARD IN CLOUD FOR DATA ACCESS CONTROL AND PRIVACY PRESERVING MECHANISM Dr. K. Sai Manoj, World Journal of Engineering Research and Technology WJERT (First Author)https://www.wjert.org/admin/assets/article_issue/35102019/1575371428.pdf
2. Protecting Sensitive Labels in Social Network Data Anonymization, Dr. K. Sai Manoj, International Journal of Modern Engineering Research (Second Author) http://www.ijmer.com/papers/Vol8_issue1/Version-1/D0801014567.pdf

3. Analysis Of Innovative Phased Array Antenna For The Space Based Applications As Per The Industrial Standards, Dr. Sai Manoj, International Journal of New Technologies in Science and Engineering , Vol. 5, Issue. 2, 2018, ISSN 2349-0780 (Second Author)

4. A Study on Data Controller-Preserving Public Auditing for Secured Cloud Storage, Dr. K. Sai Manoj, International Journal of Modern Engineering Research (**First Author**) http://www.ijmer.com/pages/Vol.8-Iss.1(Version-1).html
5. Data acquisition through telephone K.Phani srinivas , Dr.K.Sai Manoj, International journal of recent Engineering and Development October 2017 Volume 02 – Issue 10 PP 01-05. www.ijrerd.com || Volume 02 – Issue 10 || October 2017 || PP. 50-54 (Second Author)
6. Literature survey on the destruction of attaches with MH HOP to HOP to HOP-AODV Routing Protocol in Vehicular Ad-hoc Network, Dr.K.Sai Manoj, Mrudula Kudaravalli , © December 2017 | | Volume 4 Issue 7 | ISSN: 2349-6002 (Second Author)http://ijirt.org/Article?manuscript=145037
7. Analysis of Rectangular Micro-Strip Patch Antenna for Wi-Fi Applications , K Phani Srinivas 1, Dr.K.Sai Manoj2 , Mrudula Kudaravalli , International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 04 Issue: 11 | Nov -2017 www.irjet.net p-ISSN: 2395-0072 (Second Author)https://www.irjet.net/archives/V4/i11/IRJET-V4I11305.pdf

8. A Dynamic Framework of Advanced Mobile Video Streaming and Social video sharing in clouds, Dr. Sai Manoj Kudaravalli, International Journal of Engineering Research Online. Vol.5.,Issue.5,2017, sept-oct, ISSN:23217758.With an Impact Factor 5.8701, Article available online http://www.ijoer.in. (Second Author)
9. Faster content sharing over smart phone based Delay- tolerant networks. Dr. Sai Manoj Kudaravalli, International Journal of Engineering Research-Online. Vol.5,Issue.4,2017,ISSN: 2321-7758. July-Aug. Article available online http://www.ijor.in; (First Author)
10. An Efficient and Novel Approach Using T.H.E.S Methodology for CBIR, Dr. Sai Manoj Kudaravalli, International journal of computer science Mechatronics. SJIF-4.454|Vol.3.Issue .5.2017. ISSN: 2455-1910. (Second Author)
11. SOA Based CAM Cloud- Assisted Privacy Preserving Mobile Health Monitoring, Dr. Sai Manoj Kudaravalli, International journal of computer science Mechatronics. SJIF-4.454|Vol.3.Issue .6.2017. ISSN: 2455-1910. (First Author)