- `

Secure Framework Enhancing AES Algorithm in Cloud Computing

Thesis Submitted to

The Superior College, Lahore

In Partial Fulfilment of the Requirement for the Degree of

Doctor of Philosophy in Computer Science

By

Ijaz Ahmad Awan

Registration No: PHCS-F14-005

Session: Fall 2014

Faculty of Computer Science & Information Technology

The Superior College, Lahore, Pakistan

- `

Author's Declaration

I hereby state that my Ph.D. thesis "Secure Framework Enhancing AES Algorithm in Cloud Computing" is my own work and has not been submitted previously by me for taking any degree from this University or anywhere else in the country/word.

At any time if my statement is found to be incorrect even after my Graduation, the University has the right to withdraw my Ph.D. degree.

Students Signature: _____

Date: 23/06/2021

The Superior College, Lahore

- `

Plagiarism Undertaking

I solemnly declare that research work presented in the thesis titled **"Secure Framework Enhancing AES Algorithm in Cloud Computing"** is solely my research work with no significant contribution from any other person. Small contribution/help wherever taken has been duly acknowledged that complete thesis has been written by me.

I understand has zero-tolerance policy of the HEC and University.

Toward plagiarism, Therefore, I as an Author of the above title thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred/cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even after award of PhD Degree, the University reserves the rights to withdraw/revoke my PhD degree and that HEC and the University has the right to publish my name on the HEC/University Website on which names of students are placed who submitted plagiarized thesis.

Students/Author Signature: 

Name: Ijaz Ahmad Awan

The Superior College, Lahore

Certificate of Approval

This is to certify that the research work presented in this thesis, entitled **"Secure Framework Enhancing AES Algorithm in Cloud Computing"** was conducted by Ijaz Ahmad Awan under the supervision of Dr. Muhammad Shiraz.

No Part of this thesis has been submitted anywhere else for any other degree. This thesis is submitted to the Faculty of Computer Science and Information Technology, The Superior College, Lahore in partial fulfillment of the requirements for the degree of Doctor of Philosophy in field of Computer Science and Information Technology at The Superior College, Lahore.

Student Name: **Ijaz Ahmad Awan** Signature: Ij Awan

EXAMINATION JURY/BOARD APPROVAL:

Sr. No	Name	Role	Signature
1	Dr. Arfan Jaffar	Chair	
2	Dr. Muhammad Shiraz	Thesis Supervisor	
3	Dr. Usman Hashmi	Co-Supervisor	
4	Dr. Waqas Haider Khan Bangyal	External Examiner-1	
5	Dr. Javed Iqbal	External Examiner-2	
6	Dr. Tehreem Masood	Internal Examiner	

- `

Dedication

The Holy Prophet Muhammad (P.B.U.H), Who Laid the Foundations of Modern Human Civilization and Paved the Way to Social, Political, Moral, Spiritual, Economic, Cultural, Physical and Meta Physical Revolution.

- `

Acknowledgement

Major acknowledgement is to Allah Almighty, the most gracious and merciful. He is the one who enabled me to contribute a little more towards the existing knowledge. Special thanks to the Holy Prophet Muhammad (S.A.W), the TUTOR of whole mankind, whose teachings showed me the route towards development of knowledge.

I am profoundly grateful to Dr. Muhammad Shiraz my research supervisor, for his enormous guidance and positive response throughout the completion of this research work. I feel grateful to him for his involvement and I feel that I may never be able to thank him adequately for his dedication and support. Also, I would like to thank Dr. Muhammad Usman Hashmi (my Co-Research Supervisor) for his continuous help and guidance in this research work.

I would also like to thanks my parents, friends and colleagues, to whom I explained my research activities multiple times and they supported me as much as possible.

Ijaz Ahmad Awan

- `

Publications

Journal Publication:

- **Ijaz Ahmad Awan,** M. Shiraz, M. Usman Hashmi, Qaisar Shaheen, Rizwan Akhtar, and Allah Ditta "**Secure Framework Enhancing AES Algorithm in Cloud Computing**", in *Security and Communication Networks,* Volume 2020, Article ID 8863345, 16 pages **(IMPACT FACTOR 1.288).**

- `

Abstract

The world is evolving very by rapidly every passing day, and information is becoming more and more advance, changing the ways of organization's work. Basically, every organization is based on its database, and it can be said that data is the backbone of any organization. In light of the increasing importance of data for organizations, its safety from competitors and hackers has become critical. Therefore, data security has become an essential component. The tremendous growth of computational clouds has attracted and enabled intensive computation on resource constrained client devices. Predominantly, smart mobiles are enabled to deploy data and computationally intensive applications by leveraging on demand service model of remote data centers. However, outsourcing personal and confidential data to the remote data servers is challenging for the reason of new issues involved in data privacy and security. Therefore, the traditional Advanced Encryption Standard (AES) algorithm needs to be enhanced in order to cope with the emerging security threats in the cloud environment. This research presents a framework with key features including enhanced security and owner's data privacy. It modifies the 128 AES algorithm to increase the speed of the encryption process 1000 blocks per second by double round key feature. Whereas, traditionally there is a single round key with 800 blocks per second. The proposed algorithm involves less power consumption, better load balancing, and enhanced trust and resources management on the network. The proposed framework includes deployment of AES with 16, 32, 64, and 128 plain text bytes. Simulation results are visualized in a way that depicts suitability of algorithm while achieving particular quality attributes. Results show that the proposed framework minimizes energy consumption by 14.43%, network usage by 11.53%, and delay by 15.67%. Hence, the proposed framework enhances security, minimizes resources utilization and reduces delay while deploying services of computational clouds.

- `

Table of Contents

- `

- `

- `

List of Figures

- `

List of Tables

- `

Abbreviations

AES	*Advanced Encryption Standard*
IT	*Information Technology*
IS	*Information System*
PaaS	*Platform as a Service*
SaaS	*Software as a Service*
IaaS	*Infrastructure as a Service*
TaaS	*Testing-as-a-Service*
XaaS	*Anything as a Service*
AWS	*Amazon Web Services*
GUI	*Graphical User Interface*
CSP	*Cloud Service Provider*
EC2	*Elastic Compute Cloud*
HTTPS	*Hypertext Transmission Protocol Secure*
SSH	*Secure Shell*
CPU	*Central processor Unit*
SDLC	*Software Development Life Cycle*
SLA	*Service Level Agreement*
HMAC	*Hashed Message Authentication Code*
CCAES	*Combining the Chaos and AES*
IoT	*Internet of Things*
VM	*Virtual Machine*
QCSB	*Quality-Based Cloud Service Broker*
SFCC	*Secure Framework for Cloud Computing*
ASCII	*American Standard Code for Information Interchange*
IM	*Information Management*
MEP	*Medical Image Processing*
RRM	*Request-Response Model*
SP	*Service Provider*
EU	*End User*
PWA	*Progressive Web Application*

CHAPTER 1

INTRODUCTION

1.1. Overview

This chapter presents theoretical framework and motivations for the proposed research. It discusses the problem statement, states the objectives and describes the methodology used for the proposed research. This chapter is divided into nine sections. Section 1.2 Introduction, 1.3 background, section 1.4 highlights motivations for the proposed research by explaining the importance of the proposed work and significance of the proposed solution. Section 1.5 summarizes the problem statement by highlighting issues in the traditional computational offloading frameworks. Section 1.6 highlights the research objectives. Section 1.7 summarizes the methodology used in this research, section 1.8 scope of the study, section 1.9 highlights the research thesis contribution and section 1.10 sketches the layout of the thesis.

1.2. Introduction

Cloud computing is a wonderful means of outsourcing through dispersion of facilitated administrations through the Internet. The cloud is essentially a virtual server that the client can access on the web and as required premise. Cloud computing facilitates any benefit based on membership or pay-per-use that extends IT capacities permitting the client to retrieve their stored data and re-sources remotely [1]. Some of the benefit of cloud computing is demonstrated in Figure.1. Through cloud computing, IT department save money on deployments, application, security, upkeep time, expenses and improvement, while picking up from economies of scale. Cloud computing is the next generation networks which is rapidly available to update the computing globe. Generating data has increased in this information period, as well as in storing, distributing and processing requirements. These requirements are able to being satisfied by the paradigm identified as cloud computing [2]. The goal of computer security is to preserve the integrity, availability and confidentiality of information system (IS) resources through protection of the automated information system [3].

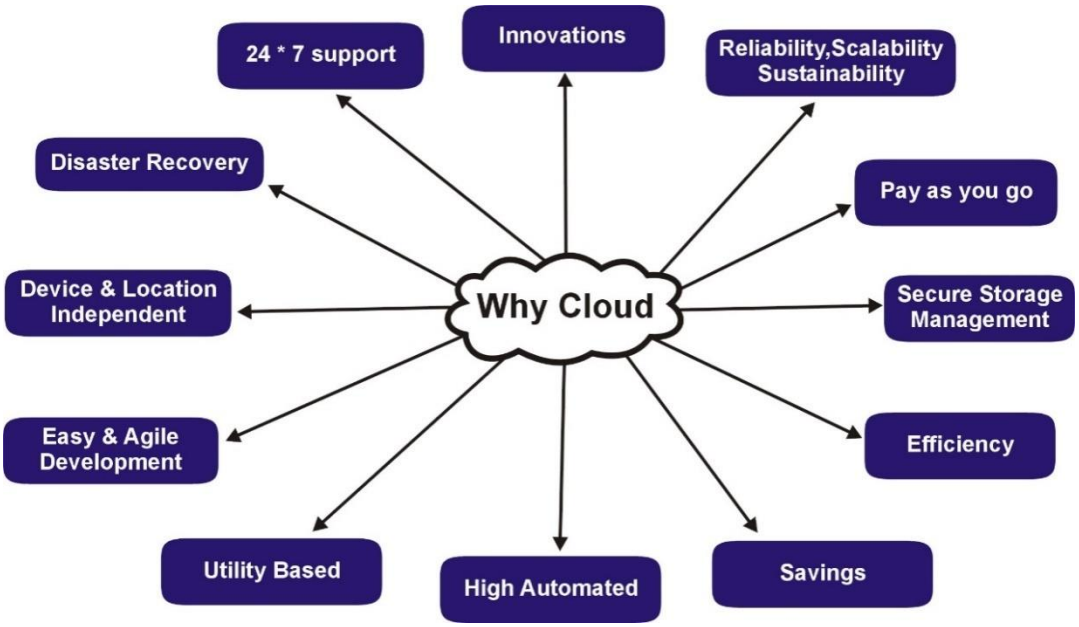

Figure 1.1: Cloud Computing benefits

Ensuring that this goal is fulfill requirement of security mechanism that include detection and preventions of computer systems. This is able to overcome the security attacks and ensures speedy recovery in the event of such attacks [4]. Cloud Computing is developing into the mainly devoted computing technology particularly as of its low cost & resource independence but as well invite a number of the most frightening concern to the expectations of this technology i.e. its security [5].

It is observed that cloud technology is used in a number of architectures, services with further technologies, and various software design approaches [6]. The models of cloud service include: 1) Platform as a Service (PaaS), 2) Software as a Service (SaaS), and 3) Infrastructure as a Service (IaaS). Architecture solutions for the public, private, community, and hybrid system depend on four cloud platform deployment models [7]. Advantages of cloud computing include flexibility, accessibility, and capacity when linked to traditional online computing or storage method [8]. However, a number of security concerns are associated with computational clouds including (i) privacy and security issues with cloud service providers and (ii) customer-related security issues [9]. In the literature, various types of attacks related to the strength of the AES (advanced encryption standard) algorithm have been proposed [10], for instance, different fault analyses which attack and introduce faults into the AES (advanced encryption standard) structure with the target to retrieving the secret information [11]. Cloud Computing is the majority up-and-coming development in Information

Technology at the present days. Cloud computing technologies can energetically supervise millions of the computer resources, and on demand allocate to a worldwide client [12].

1.3. Background

Cloud computing standard can propose some feasible practices of service area, by means of computational resources on behalf of extraordinary performance in computing applications, telecommunication services, social networking, and web services [13, 14]. In addition, cloud storage in data centers is very valuable for users just before storing and accessing their data distantly at any time without any further load [15, 16]. On the contrary, the main problem of cloud data storage is security. As a result, cloud data centers must have some mechanisms which are capable to ensure storage perfection and integrity of data that are stored on cloud [17].

Already, traditionally available methods are not able to quantify the security of cloud services effectively. Secure framework in cloud computing is a method that provides simplified management and accessing of computing resources, and a cost-effective approach is our current need. Such framework should use low power, time, and delay of network consumption with encryption and decryption that enhance the security of data in cloud computing.

1.4. Motivation

While communicating the secret information among different machine systems, there is always a risk of information privacy, honesty and accessibility. Information encryption protects information privacy and trustworthiness. Cloud computing has become the next generation architecture of IT Enterprise. In comparison to the traditional architecture, cloud computing moves the application software and databases to the large data centers, where the data management and services may not be fully reliable. Organizations have been adopting these technologies since 1990. The downside is that traditional technologies are not only slow, but they have less automation features as compared to the Cloud Computing, making it the future of computing [18].

Security concern is a major issue of the companies that are providing cloud services. This causes the blockage of the cloud computing adaptation in data management. Foremost concern of the companies is related to data security and privacy. Cloud computing is using the different delivery models and architecture of the cloud that is simulated through different sort of the service to its consumer. Different types of security attacks which has been recognized in cloud computing. The platform of cloud computing shares data and resources. Therefore, security is an important aspect. Therefore, the cloud service providers bear the responsibility of providing security as the quality of service. With many cloud services out there in the industry, customers have a challenge to choose the right one, which can satisfy their various service requirements. As traditional methods are unable to effectively quantify the security of cloud services, a new and unique method is proposed.

The proposed solution presented in this research will be simulated on platform as a service (PAAS) infrastructure as a service (IAAS). The primary goal of the research study is to provide a healthy security solution that is easily adaptable and effectively secures the cloud system. Our aim to create a new and secure framework implementation scheme for encryption by modifying the AES algorithm to increase the speed of the encryption process. It also maintains less power consumption, load balancing, trust and resources management on the network efficiently, with a complex design to keep the security level for the proposed scheme as high as possible. Solution which is presented in this has been verified and tested in real time.

1.5. Problem Statement

In the near past, the cloud computing has become popular and gaining so much attention. In the result most of the organizations throughout the world are showing interest in shifting their traditional technical system to the cloud computing system. Data privacy and security is considered as one of the major barriers in adaptation of the cloud computing technologies. Due to these security concern, some organizations do not want to shift their data from the traditional computing environment to the cloud computing environment. In order to ensure data security and information in the cloud computing number of tools and techniques has been developed in the recent past. Most of these techniques are still not adopted by the cloud computing service provider.

Existing security systems employ one or two attributes at a time, i.e., low security and more time consumption to encrypt/decrypt the data. This makes the process more time-consuming and therefore increases the network use, power consumption, and delay in the network [19,20,21,22,23]. Cloud computing is that kind of platform which shares the data and resources efficiently, and therefore, security must be provided to the users as security is an important aspect of cloud computing. So, this is the responsibility of the cloud service providers to provide security with all attributes, such as less power consumption, delay of network, and time consumption [3,24,25,26,27,28,29]. Already, traditionally available methods are not able to quantify the security of cloud services effectively. In this context, a new security system is needed that enable cloud resources to be used efficiently by costumers without exposing their sensitive data and private information to unauthorized entities including the cloud providers. Further, the data owners should be able to control their outsourced data security and privacy, and verify security conditions, such as the integrity of the data.

Secure framework in cloud computing is a method that provides simplified management, assessment of computing resources and a cost-effective approach is the need of the hour. The framework should use low power, les time, and delay of network consumption with encryption and decryption that enhance the security of data in cloud computing.

1.6. Research Objectives

We aim to propose a secure framework for data security in cloud. The following are the objective of the research:

- To identify the challenges of security associated with the adoption of Cloud computing and enlist the existing cloud computing challenges that have no mitigation strategies defined earlier and find out their solution from the literature.

- To study the technique approaches for cloud computing security of over network in Cloud using proper authentication, integrity and confidentiality.

- Propose a framework in computational Cloud based on technical and non-technical aspects in order to secure data and evaluate the proposed framework,

by using both mathematical model and simulators. To authenticate the framework by developing it with latest techniques. The propose framework should be use low, power, time and delay of network consumption with encryption, decryption that enhance the security of data in cloud computing.

1.7. Proposed Methodology

Keeping in view the previous literature more research work need to done in cloud computing, and for this purpose we studied all the challenges and their proposed solutions. There are different kinds of aspects in security of data likewise data integrity and availability. There are many customers who don't relay on security and privacy of cloud computing. That's why companies are showing least interest in moving their private data on the cloud platform. The core of the problem is insecurity of data. In order to solve the problem in effective way by making variety of measures. Our research target is to facilitate with the solution for the threats that face by customers while adaptation towards cloud services. For this purpose, a framework should be proposed for implementation of data and information security in cloud environment. It will protect user's data, messages and information against various attacks.

In this study we explain, the data integrity aspect of data security and working on a development of secure, cost effective and a framework for remote data integrity in computational cloud. To evaluate the proposed framework, we will take help from both simulators and some mathematical models.

1.8. Scope of the Study

Implementation on design of Secure framework in cloud computing is a method that provides simplified management, accessing of computing resources and a cost effective approach is need of the hour. The framework should use low power, less time and delay of network consumption with encryption and decryption that enhance the security of data in cloud computing.

1.9. Thesis contribution

The thesis contributes towards the design of the security framework by implementing a new scheme of encryption/decryption. It also determines the serious components of the security framework within the cloud computing community. It would be helpful for

those cloud users and cloud service providers who have similar requirements in terms of security during implementation. The framework helps in faster computing with lesser power consumption, network usage and reduced network delay due to the smart algorithm. The framework employs a symmetrical encryption method to provide trust to users and enables trusted gateways. The proposed framework includes the key features including enhanced security and owner's data privacy. It modifies the 128 AES algorithm to increase the speed of the encryption process 1000 blocks per second by the double round key feature. However, traditionally, there is a single round key with 800 blocks per second. The proposed algorithm involves less power consumption, better load balancing, enhanced trust and resource management on the network.

1.10. Layout of Thesis

Chapter 1. This chapter deals with the research work overview, introduction, problem statements and research methodology.

Chapter 2. In this chapter detail discussion on cloud computing and its architecture is done. Different service delivery and deployment models of cloud computing which highlights the benefits, trust, cryptography, security issues and challenges is presented here. The chapter also discusses the different approaches in addressing cloud security issues and challenges. In this chapter provides a literature review based on related work that overcome risks of cloud computing and the various other industry standards. This framework provides strategies for implementation of security in management of information. Literature review that highlights the existing security and privacy solutions.

Chapter 3. This chapter explain the development of framework related to security that is the main key for identification, evaluation and analyzation of cloud environment. It explains the architecture of proposed framework, and distinct operating procedures of the proposed framework for the operating modes of accessing the services of cloud server node. The researcher will present the new scheme by show the modified algorithm. The chapter also presents in detail, the segregation of cloud architectures into layers. This segregation highlights one of the original contributions to knowledge.

Chapter 4. In this chapter results of new scheme will be discussed. It includes test vectors for new scheme compared with original scheme then test speed of new algorithm. It also deals with speed of original algorithm then the security tests will be compared with other security tests for modified algorithms.

Chapter 5. The summary of research study and work done to achieve the aims and objectives raised in the study is discussed in this chapter. It explains the findings of the research work, highlights the significance of the proposed solution, states the limitations of the research work and proposes future directions of the research.

CHAPTER 2

BACKGROUND AND LITERATURE REVIEW

2.1. Overview

This chapter discusses the basics of cloud computing technology and its correlation with security and privacy in cloud computing services. This appreciate the concept which is applicable in different services and deployment of models. These models are benefit to identify the security problems in renewed technology. It describes cloud computing's characteristics key and development of its concept in section 2.2, describes the cloud architecture, its service delivery, deployment models, Cloud Computing Components, Cloud computing enablers and Cloud Service Provider. 2.3. Need for data security in cloud and 2.4 cryptography. Section 2.5 and 2.6 discusses security issues and challenges of cloud computing. Section 2.7 discusses Privacy, Security, Trust Issues, challenges of cloud computing. In 2.8. trust in cloud computing and 2.9 Trust management techniques. This section 2.10 consists of present related work about the cloud computing security, privacy, trust and the other presents related work to the available lightweight cryptographic systems. Out of these, a few of them are presented here and 2.11summary of the chapter is given in the last section.

2.2. Background

Cloud computing came forth as a new distributed computing model and a new era of computing began near about 2008. The new comers elevated insight very well in this field. The word cloud has become a symbol for the internet and it has also obtained more popularity now. In cloud computing the term "cloud" be able to point at different types of networks, hardware, storage, services, and interfaces as a combination of computing services provided to the users. Cloud services comprises of giving such kind of infrastructure that helps the users to get the computational resources on demand over the Internet. Hence it indicates the Internet-based computing services such as storage, servers, and applications [30].

Cloud Computing allow us to share out the necessary information, resources, and services. The computing has been made very much efficient by Cloud Computing by centralizing bandwidth, processing and storage. Different types of mail application like Gmail, rocket mail, live mail etc. are its examples. To send your emails, you just have to get connected with internet. To provide privacy and security, Cloud computing is also used on demand basis. The most appropriate use and advantage is to assist the users that they do not need to purchase the computing resource they need from third party wholesaler; therefore, cloud helps the users to save time and money [31].

2.2.1. Characteristics of Cloud Computing

The following are seven essential characteristic of cloud computing [32].

- **Abstraction:** A cloud domain conceals the computational data and information from the clients and programmers. Clients even do not know where their calculation has been completed. Nevertheless, their calculation should be completed using enrolled resources only. As the abstraction level increases, basic execution must be less to know.

- **Virtualization:** In cloud computing, virtualization is the formation of a virtual (as opposed to genuine) adaptation of hardware, working framework, and storage devices or system resources. In a distributed computing environment, virtualization can be accomplished by asset pooling and asset sharing to make assets very adaptable.

- **On demand self-service:** A client can be run, observe, and deal the services which are automatically given by the resource provider organization without the assistance of client association. Computer services, for example, email, applications, system or server administration can be given without the assistance of client connection with the resource provider.

- **Broad network access:** A client can access cloud services and resources delivered by a service provider using the client platform accessible over different devices. Resource Pooling: For serving computational services and resources to numerous

clients, services are shared utilizing a non-dedicated way so that virtual resources dynamically allocated and reallocated by the client request. Cases of computational resources are information and data storage, arrange transfer Speed, virtual machines, processing, physical memory.

- **Rapid elasticity:** In cloud computing it can be defined as the ability to provide scalable resources within no time. This is automatic and to the users it is seemed to be unlimited resources. Scalable resources can be defined as ability to alter the allocated resources to the client in order to meet the current demand.

- **Resource pooling:** In cloud computing environment, multiple clients are served by allocating or real locating the resources depending on the demands. Resources are may be virtual or physical in the pool that is assigned to the clients. Resources we discuss are storage, computation and processing power, memory or network bandwidth etc.

- **Measured services:** As the name suggests service provider measures the services provided to the clients. This may be done for various reasons that may be billing or reallocation on the basis of previous record of resource used so that can predict about future need to some extent or making the use of resources effective etc.

2.2.2. Cloud Computing Service model

Many different services can be classified into various categories. The customers can access online services by using cloud computing for example different software. In this way, there is no need to install different applications on the client's machine. Such kind of delivery model is called SaaS. (In PaaS delivery model, client can build up different software and applications). Some other types of delivery models are; Infrastructure-as-a-Service (laaS) which provides platform for applications and networking environment, Testing-as-a-service (TaaS) provides an environment that is used to test different applications and the lost one is Anything as a service (XaaS). [33].

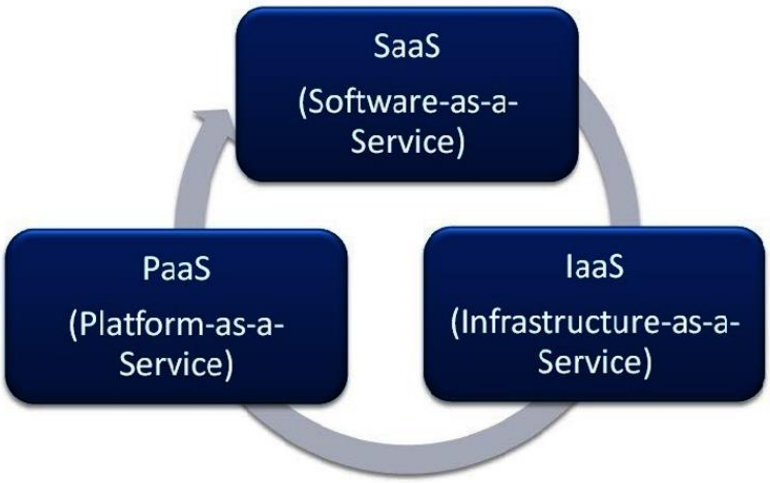

Figure 2.1: Cloud Model Services

- **Infrastructure as a service (IaaS):** It is the provision given to the clients to use the resources such as processing power, storage, network etc. Clients are provided with the facility to run the arbitrary software which includes operating systems, storage and different applications. They are not allowed to access the basic infrastructures of the cloud but have only access to operating system, storage, limited networks and applications. It is the most basic cloud facility provided to the clients, which includes virtual setup and computing infrastructure. The bill is given against the services provided by the cloud, how much resources are allocated and consumed by the customer. IaaS examples are Amazon EC2, Flexiscale, Rackaspace Cloud, GoGrid, Joyent Cloud etc.

- **Platform as a service (PaaS):** It enhances IaaS by providing development and programming model. It is the service provided to the clients to deploy their own created software applications on cloud infrastructures using the programming languages, tools, services or libraries. The clients do not have access to the alter cloud infrastructure but has all access to configure or control their own developed applications.

  It is purely a development environment that facilitates the application developers by giving them access to libraries, programming language execution environment, toolkit, operating system, data base, web server etc. It provides ease to developers to run their software on clouds without buying and hardware software that meets

their requirements. PaaS examples are Google App engine, Microsoft Azure, SalesForce (Force.com and Heroku), Amazon Elastic Map Reduce and Aneka etc.

- **Software as a service(SaaS):** It is the service provided to the clients to use applications running on the cloud infrastructures. These applications can be accessed from various node points such as mobiles handsets, Web browser, application software, any program interface etc. The clients only have some specific access to manage it for example Emails, one can manage his account, update his profile, use it to send messages etc but not able to manage the storage, network, operating system, servers etc. A specific user interface is provided to use the applications. Examples of SaaS are Microsoft Office Live, Salesforce CRM, Google Docs etc.

2.2.3. Cloud Computing deployment models

Cloud model has four deployment models Before proceeding towards the deploying of the cloud computing solutions one must know about the type of the cloud. According to the need of client, type of the cloud is to be used. One must be clear about the properties of cloud according to his need. Selection of appropriate cloud is very essential. Some of types of clouds are discussed below [33].

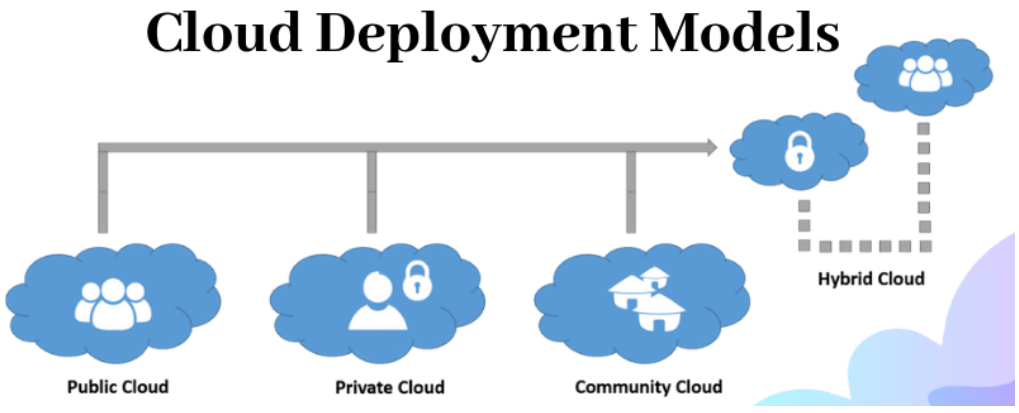

Figure 2.2: Cloud Computing deployment models

- **Private Cloud:** It is the type of cloud which works exclusively for a client, created, managed or operated by organization itself or third party. As it works purely for one client so it cannot combine or shared with other customers. It

provides more secure, managed and controlled environment with greater performance and reliability but costs high comparatively.

- **Public Cloud:** When cloud services are available publically or free then this is called public cloud. Architecture of public cloud is similar to the private one but it may differ in some aspects such as privacy, security and confidentiality etc. for the services (computing power, storage, applications etc.) provided to clients. Public clouds are mainly managed, operated and owned by some business, academia or government organizations. Common examples of public cloud service provider are Google and Amazon Web Services (AWS). They provide storage space to the clients through internet.

- **Hybrid Cloud:** Hybrid cloud is the combination of the more than one deployment model i-e private, public or community. This is flexible enough to provide the properties of each cloud. Due to this we cannot mark boundaries among them as public, private or community. It provides more security and control or manage applications as compared to private clouds. They are usually managed by public cloud service provider.

- **Community Cloud:** It is designed for a community that have common objective to use the cloud. It can be controlled, managed and operated by community itself or third party or both.

2.2.4. Cloud Computing Components

Cloud computing architecture is based on three basic components. These are front end (clients), back end (storage) and network. The whole cloud computing setup is based on it. They are explained below [32].

- **Clients:** The clients are those who demand for the services of cloud computing (storage, processing and computational power etc.) through cloud service provider. They include thin clients (desktop virtualization environment), thick clients (computers and laptops) and mobile clients (smart phones, tablets and iPad etc.).

- **Network:** Cloud network is the backbone of cloud computing environment as the whole structure relies on it. It usually offer a connection that may be internet, intranet and inter cloud. Cloud service provider, servers, data centers and clients do their communication through it.

- **Data centers:** Data centers are cloud storage. They are consisting of servers that offer large space to store and manage data. This is online storage that is accessible to clients. Clients may get illusion of unlimited resources and storage as this is virtualized setup. This is geographically distributed to serve all clients across the world.

2.2.5. Cloud computing enablers

Cloud computing is supported by many technologies. Enablers of cloud computing are virtualization, multi tenancy, web services and cost effective hardware. Advancement and combination of these results in cloud computing. They serve as the backbone or initial support to the developers [34].

- **Virtualization:** It is very important in the cloud computing. As it allows us to make multiple mirrors of the physical computer setup. This enhances the computational power of the system. The physical resources of the computer are divided and dynamically reconfigured as needed. This provides efficient use of resources and scaling up of it in order to meet the demand of applications.

- **Multi tenancy:** As the name suggests it offers access to multiple clients to use same resource without interfering each privacy or space allocated to them. Optimal use of resources is main objective.

- **Web services:** This is software base setup that allows machine to machine communication over the internet. Many cloud service providers make their own GUI of applications integrated with web services as by default this has no GUI interface. This is independent of machine configuration or any other components of it. This provides a standardized platform to gain access of different functionalities for example XML, WSDL, SOAP etc.

- **Cost effective hardware:** Hardware cost and speed of processing have inverse relation. As in past few decades' technology is improved a lot. High computational power servers are installed in small area which provides us parallel computation speedily and accurately.

2.2.6. Cloud Service Provider

Cloud services are provided by cloud service provider (CSP). The few of the best CSPs are discussed below [35,36].

- **Amazon web services:** It is considered as pioneer in providing clouds services launched in 2006. It includes Elastic Compute Cloud (EC2), and the Simple Storage Service (S3) and on demand storage capacity. It similarly delivers services as Simple DB (a database Web service), the Cloud Front (a Web service for content delivery) and the Modest Line Service (a hosted service for storing mails as they mobile amongst nodes).

- **Microsoft azure:** Microsoft company launches Microsoft azure in 2010 to provide cloud computing services to the end users. It allows users to access many of the Microsoft online services such as Live, .Net, SQL, SharePoint, and Microsoft's Dynamic CRM.

- **Google cloud platform:** Google cloud establish in 2011. It provides networking, computation, data storage, big data management, data transfer, API platform and ecosystem, management and developer tools etc.

- **IBM cloud:** IBM launches its cloud services in 2013 and provides many services to the users that are computation, networking, storage, data management security, analytics, AI, and many more.

- **AT&T:** AT&T provides cloud services that are collocation services, cloud networking, content delivery network, disaster recovery, virtual data center, cloud content management.

- **Rackspace:** It is founded in 2006 as a set of cloud computing services and products, charged on the basis of utility computing model. Services provided by

Rackspace cloud are Cloud servers, Cloud files, Cloud sites, database, backup and monitoring. There are six data centers that provide these services globally.

2.3. Need for Data Security in Clouds

The basic requirement of data protection is security and it must be implemented by cloud computing system specifically or generally by the Information Technology System. The cloud service providers perform security mechanisms for user needs. There are three main requirements for security which are confidentiality, integrity, and accuracy of data.

Cloud computing is the most oriented field of information technology. Independent user's social media and its related structures shifting towards the outstanding filed of cloud computing. Therefore, cloud goes through know of any issues. In the development of data these issues cause problems. In cloud computing data is stored in remotes which are note under the users control. So, the data on cloud computing is approach from everywhere and it is easily susceptible. Still the remotes server is not trustful and easily cause misuse and delete of data. Even through cloud architectures has its own security, so it is essential.

Typical cloud computing has particular security architecture along many customers with multiple demands. In this situation, adjustments on services of cloud computing is not possible. It makes sure data should not be manipulating by cloud server. In cloud computing storage of data and its security is ensured by the core security. So, it is essential to compute security proceeded at the end of users. Most people believe that data is safe in local storage, but some others believe that external data is more safe because external companies are more responsible for data and they do not have any concern with your data.

2.3.1. Key Components of Data Security

- **Availability:** Data availability make sure protection of data even through guard the data in any natural mishap or human fault such as fires or power out.
- **Integrity:** Data integrity granted the data management in its core state will not be transformed intentionally or accidentally altered.

- **Confidentiality:** It means data is available or operates only by authorize individuals is core processors.

- **Traceability:** it means data genuine should be confirmed by both users, for the protection of data issues.

2.4. Cryptography

Cryptography is the method of modification of message i.e code or ciphers of original message for secure communication between one user to other user. A cryptography algorithm is a service of mathematical function and fixed collection of steps to perform encryption and decryption of original message. For this purpose, two basic activities are performed one is encryption and other is decryption. Cryptography have unique characteristics to keep encrypted information secure on cryptographic algorithm, which produced results of previously encrypted information. The main purpose of cryptographic algorithm is to ensure decryption the cipher text without help of keys [20,22].

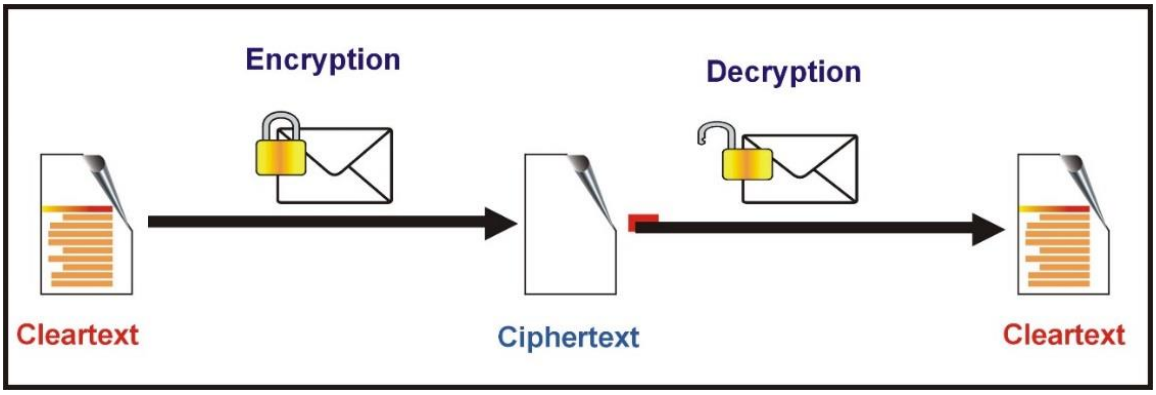

Figure 2.3: encryption and decryption process

2.4.1. Encryption

The transformation of data into other form. Which express as random, meaningless and unintelligible. This process is occurring by the help of secret encryption keys and cryptographic cipher. In other words, encryption is the method of conversion plaintext into cipher text. In the process, input is in the form of plain text and the output is in the form of cipher text. This is the collection of cryptography; encryption is the most appropriate way to get data security level.

2.4.2. Decryption

Decryption is the mechanism to charge the encoded data into intangible form. It is decryption process to change cipher text into plaintext. For this purpose, input of decryption process and plaintext is the output of decryption mechanism. This process is impossible without the help of correct key.

2.4.3. Goals of Cryptography

- **Confidentially:** It is the system of security information and only the authorized person can access it. Confidentially, is the process of transition of data by passive actions. Different steps of security, detection and discover by the content of data. The extended services manage all the continuous and data transition among users over a period of time. The purpose of confidentially is the protection of traffic flow by analysis. The main requirement of it is to rescue the communication network and traffic flow by the unable attackers to observe the frequency, destination and its length [23].

- **Integrity:** It safe the information by not altered the data by any unknown source. It should have ability to detect the data manipulation by unknown authority. Data manipulation include data detection, substitution or insertion [23].

- **Authentication:** It provides services related to detection. Data authentication gives data security and it is applicable to both entities and information. this is because two parties take part into traffic should know each other. And the delivery of information through a channel should be authorized as the data content and data basic.

- **Non- Repudiation:** Non repudiation protect either sender or services from execution of an information. Therefore, when the massage is sent, the receiver has proof that information from the suspected sender. As it is when data is received by the sender have proof about suspected receiver [24].

2.4.4. Cryptographic Techniques

2.4.4.1. Symmetric Key Encryption

Symmetric key encryption operates only one key for both encryption and decryption process. The key has transformed to both sender and receiver before the mechanism of encryption and decryption. In symmetric-key encryption the encryption key can be message from decryption key and vice versa. The secret keys play essential part is its strength that depends on the length of key. The application of symmetric-key encryption is highly productive. So customers did not outcomes of encryption and decryption process [24].

2.4.4.2. Asymmetric Key Encryption

Asymmetric Key Encryption involves a pair of keys, a public key and a private key, associated with an entity. The respective private keys are also called secret key. It encrypted data and decryption with private key [24].

2.5. Security Issues in Cloud Computing

Cloud computing contains applications, platforms and infrastructure sectors. All sector performs unlike operations and deals dissimilar products for businesses and individuals about the world. There are several security problems for cloud computing as it includes numerous technologies. The given below are a number of security concerns in a cloud computing environment.

- **Data Security:** Hypertext Transmission Protocol Secure (HTTPS) and Secure Shell (SSH) are the maximum mutual acceptance in command to promise the material security and statistics truthfulness. The cloud earners like in Amazon, the Changeable Cloud or EC2 commissioners are fixed not have admittance to use cases and so cannot log into the caller functioning organization. So, they necessity cryptographically robust SSH answers in command to improvement admittance to a congregation [37].

- **Data Availability:** The information proprietors agonize in organization disappointment of the capability wage earner once the facts are reserved for isolated

systems owned by others. If the service of the clouds enthusiasts obtainable of the act, then the facts will convert unattainable as it is contingent on a sole deal worker [38].

- **Data Transmission:** Popular data shows the encryption technique that is recycled. Now the Secure Opening Level procedures are used. The data only goes where the user wants this woman to send using authentication and the information not reformed through the show. The cloud wants the data to be encoded since it is no coded through dispensation [39].

- **Data Location:** The careful placement of the datacenters is not acknowledged to the cloud and they do not have slight regulator done admission to their data. Well-known cloud wage earners have datacenters all finished the world. So, in numerous a suitcase, it's a matter. In facility to sanctuary truth in statistics is a cloud like spread organization, the contacts amid diverse data sources need to be controlled or handled correctly and starved of harm. The essential comprehensive business executive ensures [40].

- **Server and Application Access:** The directorial contact in cloud computing is conducted via the Internet; it is more disposed to revelation and risk. It is self-same significant to limit these admissions to statistics and try to check this admittance in instruction to preserve perceptibility of variations in organization over nor. Due to these strategies, some of the personnel will not give admittance to a convinced total of data. Consequently, these security plans ought to be obeyed through the cloud in instruction to avoid malicious interruption by unlawful users [41].

- **Data Access Control:** Sometimes familiar leak can be illegally accessed due to lack of secured lowdown coming oversee. Perceptive information magic charm haziness computer surroundings become visible as a most important tissue with astounding to brilliant approve of contact a cloud-based system [41].

- **Data Integrity:** Data integrity contains the persistent cases as human faults occurs in report is entered. During the transformation of data form one computer to other

errors may appear. Distinct faults originate in malfunctioning of hardware like in disk crashes, software bugs, viruses blank and viruses [40].

- **Security issues in provider level:** A mistiness is opportune reserved when learned does the vendor provide a well-suited ambition to the customers. The provider should make a good reverie layer through the customer and user. In addition, should drive actual that the server is in fact secured from uncut the external threats material may be present across. The most computing boost provider has [42].

- **User level Issues:** User must know that because it is his own work, that there should not be a loss of any kind of data or theft of data for other users who are using the same Cloud [42].

- **Infected Application:** Service contributor has to make a clean breast the massive admittance to the server restrain plenary rights for the report of monitor and continuance of headwaiter. Therefore, this determination ends several detestable clients from uploading division-dirtied purpose onto the fog, which will exceedingly change the customer all over again murkiness compute abetment [42].

- **Virtual Machine Security:** It is the chief mechanisms of the cloud. Virtual apparatuses are active. It ensures that examples affecting on the comparable machines are isolated from each other and that is a key core of virtualization. They can also be impeccably moved between worldly waitpersons and can be cloned. Virtual Machine Screen is a software, which tries to abstracts the physical hardware when it is applied by virtual apparatuses [43].

- **Network Security:** Sniffer DNS attacks and including reuse IP address are the issues related to network security. Applications in sniffer attacks are responsible for pickup packets in network. In the DNS domain name change into IP address is not the secured system. Its users are forwarded to other malicious cloud rather than are which is asked for [43].

2.6. Cloud Computing Security Challenges

Cloud computing research addresses the challenges of meeting the requirements of next generation private, public and hybrid cloud computing architectures and also the challenges of permitting applications and development platforms to take improvement of the welfares of cloud computing. A lot of existing issues have not been completely addressed, while new challenges retain emerging from industry applications. Some of the challenging research subjects in cloud computing are given below.

- **Security:** It is understandable that the security things have frolic the in general filled of beans individual in deter cloud computing receipt. There ensues no unwillingness that drumming your data, consecutively your software on superstar else's hard disk by income of somebody else's CPU looks threatening to countless. Well-known security difficulties such as data injury, phishing, bot net (successively at all on a collection of attacks) location strict doubts to management's facts and software [44].

- **Data Integrity:** Data honesty is a statement that information difference only in reply to standard infrastructure. For container, if the supporter is responsible for raise and corroborate evidence interrogation and the member of staff serving at bench executes them blindly, the interloper will for all time be talented to adapt the client-side cipher to perform what he has authorization to do with the backend record. More often than not, the interloper is able to read, modify, or delete data at determination [44].
- **Availability:** Numerous operators and customers need admittance to cloud services at slightly time, which numerous businesses if cloud facilities are not accessible at slightly time [31].

- **Risk of Seizure:** In a civic cloud, you are allocation-computing income with preceding business. Educational you're in sequence in a condition of ring up open with former business could litheness the government "realistic motivation" to capture your property specified that further acting ballet company has despoiled the instruction. In a minute as your piece the surroundings in the cloud, capacity place data at risk of requisition. The only defense moving the introduction of seizure for a member of personnel is to agenda their statistics [31].

- **Data Location:** As soon as the user kinds use of Cloud computing facilities, do not comprehend this question that data is deposited in which place and the provision is positioned in pardon place [33].

- **Constant Feature Additions:** Cloud applications experience endless article trapping and user keep hold of up to date with submission enhancement to be clear-cut that they are safe. The speediness at which requirements will transform in the cloud will contact in cooperation the SDLC (Software development life cycle) and safekeeping [33].

- **Losing control over data:** Subcontracting income-losing important regulator over statistics. Great have an account do not scarcity to sprint a program on cloud nine in the cloud that danger conceding their data over communiqué with regarding the previous program. Amazon unassuming store Service (S3) APIs make accessible collectively storage place- and article height right of entry wheel, with evasion that no more than article confide admission by the storage place and/or entity instigator [37].

- **Service Level Agreement:** Even despite the fact that cloud customers send out not receive it be in charge of over the original computing capital, they do proclivity to coordinate the excellence, accessibility, uniformity, and presentation of the currency what time consumers comprehend migrate their command center vitality function onto them entrust cloud. Classically, these are providing from beginning to end overhaul misuse agreement (SLAs) negotiate linking the provider all over again customers [40].

- **Authentication:** Authentication: All over the internet, the tidings stored direction the smog by the user is painless unauthorized family. To ensure the straight forwardness of data, the user should substitute able to dispose the what drawing near logs to arrange that proper plain users are producing to nearing the data. The user itch provide that the cloud provider is taking all the security measures through the protection of the message [40].

- **Recovery:** If the center of server data of service provider, it is the cause of some natural or unnatural problems, then it is important to inform cloud service [45].

- **Incompatibility Issue:** Storage facilities provide by solitary cloud supplier possibly will be incompatible with additional vendor's military would you prefer to transport as of one to the supplementary. Vendors have acknowledged for generating what the present world calls "sticky services" – military that a termination customer may have endeavor stirring on or after one cloud vendor to the alternative [45].

2.7. Trust-Based Privacy, Security, Trust Issues and challenges in Cloud computing

2.7.1. Trust-Based Security and Privacy Issues

Security and privacy are two main but very authoritative features of any technology, which provide to the operators of cloud computing, which his nowadays days distributing with a lot of concentration on the two factors whether provider or not provide services. In this stage, we concisely describe all issues of security and privacy of cloud computing contributions.

2.7.1.1. Privacy Issues

There are a lot of confidentiality hazards are available in the field of cloud computing, which related to privacy cause fluctuation permitting in cloud services.

- **Lack of control:** We believe cloud computing gives us safe Technology, which can deliver the abilities to remove our data and software program of the solitary amount and created by the complete system, which works more than one that can handle the heterogeneous form of masses [46].

- **Unauthorized distribution of data:** There are so many risk factors in the agreements and legal terminologies regarding cloud computing data distribution. Data may be distributed to the companies for unauthorized access because there are not any legal terminologies given in the agreements, if the cloud company is acquired by another company or for some reason cloud company becomes

bankrupt then there is not any guarantee, which purposes the new company will use the data [47].

- **Risks over data transfer:** Through cloud computing access service and users between can cloud-based services via remote servers. So the connection between customers and service providers is always not protected.

- **Software-based fault isolation:** the binary translator uses singular protectors to protection that lone demand and public library code is understood, that code cannot leakage the two-fold explainer, that no inoculated code on the elevation and on the mountain is completed, and that completely system demands are shown to the interposition framework [49].

- **Policy-based system call interposition:** the system demand interposition framework confirms that entirely system desires are check and authenticated and that merely official system requests are implemented. A policy gearstick which influences and which program positions are permitted for respectively separate structure demand [48].

- **System for the real- time:** The dynamic investigation of hateful Windows means drivers. dAnubisbe able to mechanically deliver a high-level, human-readable statement of a driver's performance happening the system. We functional our organization to a dataset of over 400 malware models. The consequences of this analysis outbuilding approximately graceful on the conduct of kernel-level malicious encryption that is in the rough today [49].

2.7.1.2. Security Issues

Nowadays in cloud computing, the security frame factor is the chief and vital factor to build a comprehensive relationship amongst the user and service provider [5][6][50].

- **Risks of data accessibility:** Data accessibility is a very critical problem in the cloud computing systems, we know when we are using cloud services, our data has stored on the cloud servers, which are located in the dissimilar spaces of the world [51].

- **Multi-Tenancy with Virtual Machines:** To deliver the cloud computing services to customers, with multi-tenancy architectural, the service provider vendors practice means organization and job development mechanisms, in which software's are planned for the virtualized distribution of work freight on the different apparatuses so that each organization can practice the customized virtual resources [52].

- **Availability and backup of data*:*** Currently we pursuits all business sectors to improve the capabilities of work to shuffle with cloud computing services, though there are approximately chief issues of cloud computing services backups and data recover possibilities [52].

- **Cloud Audit:** In the present-day cloud auditing has grown into popular service that each organization desires to practice to increase the review correlated capabilities. But the requirement of cloud service provides to make the internal audit monitoring controls relatively than peripheral monitoring controls [53].

- **Copilot can monitor main memory:** The Copilot display prototype has confirmed to remain an active kernel integrity display in assessments in contradiction of 12 communal kernel-modifying rootkits. In its avoidance conformation, the Copilot display prototype that is able to identify modifications to a cloud kernel's text, LKM text, or scheme demand course within 30 seconds of existence complete through a rootkit [53].

2.7.2. Trust Base Security, Privacy Challenges

Security, Trust, and Privacy are the three important concerns about cloud computing. In the cloud computing world, the virtual atmosphere contracts consumer contact computing influence that surpasses that controlled inside their physical world. Already evaluating Security apprehensions of Cloud Computing we will surprise our conversation by important Security, trust and Privacy [54].

2.7.2.1. Trust Base Security challenges of Cloud computing

Cloud computing is not protected by naturally. The Security hazards are determined in the cloud services and distribution model. The security challenges connected to Cloud computing were discussed in detail [55].

- **Users control over Cloud resources:** Unfortunately, Cloud operators have no proper mechanism to complete the Cloud resources. Here is a hazard of data to the third party on the Cloud or the Cloud supplier [51].
- **Data confidentiality and secrecy:** Encrypting data is a mutual repetition to defend the confidentiality and privacy of data. End-users can grasp the decryption solutions can be approximately technical experiments.

- **Use of the data & data access control:** The cloud computing needs the uniqueness and contact regulator organization procedures. Before data are transfer to a third party for the management or storing inside a mutual operator environment, safeguard necessary be engaged to confirm continuous and complete regulator of the data [56].

- **Application & Platform Security:** Today, the presentation, that was established for interior usage and animation recycled in a cloud computing environment deprived of lecturing the hazards of different technology [52].

2.7.2.2. Trust Base Privacy challenges of Cloud computing

In the Cloud Computing environment, Cloud suppliers supply vital data, records and registers of Cloud users. It is challenging for corporations and private users to regulate the data while they commend to Cloud suppliers. Approximately key confidentiality encounters as specific to the Cloud-computing background are: [54].

- **The sensitivity of information:** Some kind of information can be presented, or achieved by the Cloud providers. The statistics might be extremely trustworthy or exceptionally appreciate as corporation benefits.

- **User's right to access the data:** The workers of similar Cloud share the properties of data treating and the data storing amenities. They are unprotected from the hazards of figures, material trickle, moreover by the unplanned or accidental, act. [55].

- **Data transfers to different locations:** Uncertainty the data on the Cloud modification in multiple positions, it is difficult to look at the data transfer. Data transmissions in additional states involve preparations to locate. [51].

- **Externalization of privacy:** Corporations charming in Cloud computing is that the privacy guaranty they have finished concerning their regulars, employees or additional third events will remain to relate with the Cloud computer benefactor [56].

2.7.2.3. Trust challenges of Cloud computing

Trust is an unjustifiable obstacle that essential to be approved. Cloud customers' duty to faith the cloud providers. Suppliers essential trust regulars with admission to the services which might mains to security subject [57].

- **Joining the Cloud by users/resources dynamically:** In cloud computing location many operators or possessions are connected and leave cloud animatedly. Operators, assets, and cloud must be establishing the trustful association amongst themselves [51].

- **Different Security policies:** The cloud background contains distributed operators and has properties of different confined schemes, unlike security strategies.

- **Continuity and Provider Dependency:** The defect in Cloud structural design and the absence of clearness will grow the security risks. In the number of Cloud operations, the federal organization and control the present some solitary opinions to controlers[56].

- **Compliance with applicable regulations and good practices:** When appropriate commandment to Cloud service of the firm, the sponsor will necessary to obey other

protocols such as privacy, Universal civic law agreement law and Customer security law, etc. [51].

- **Trust enhancement through assurance mechanisms:** The Cloud-computing provider cannot assurance the resistor of the Cloud workers finished their possessions. It is need of time, the formation of suitable “payments and reins” to determine that Cloud workers encounter their responsibilities and develop their capacities as Cloud operators [52].

2.8. Trust in Cloud Computing and Technology

Trust is an arrangement of considering isolated the uprightness, truthfulness, self-belief, competence, reliability, privacy conserving, etc. This object being relied on the service furnished. Consider organization will have powered be situated defined by way of "a perception this is stimulated via an individual's approximately convinced crucial device structures". Few kinds of research evaluate device accept as true with primarily founded by documentation of articles, such as records concealment, facts integrity, unsanctioned get entry to hindrance, invention best dependability, provision accessibility and steadiness, arrangement safety, contract anticipated period, hazards control crucial conditions, and so forth. Trust in Cloud Computing and Technology are shown in Figure 2.4 given below [50,46].

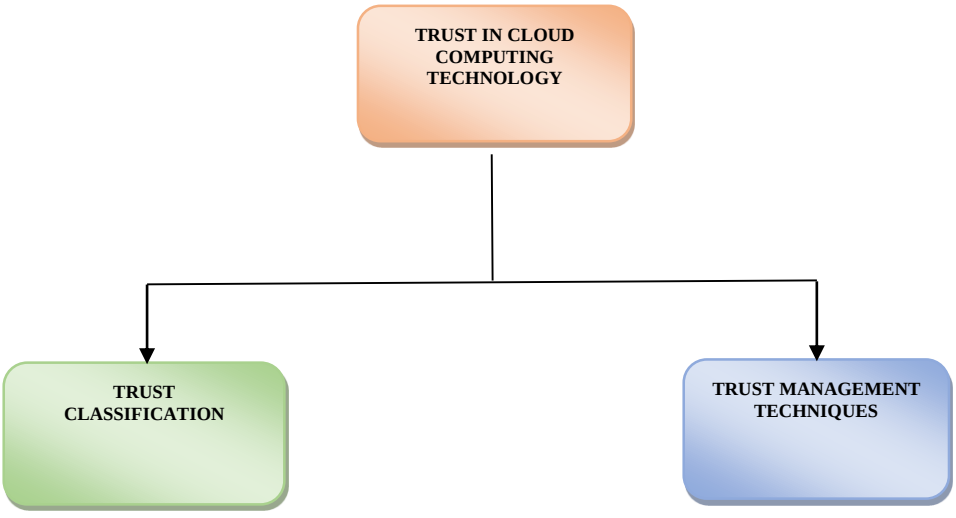

Figure 2.4: Trust in Cloud Computing Technology

2.8.1. Trust in Cloud Computing Technology

The introduction of the paper states, some of the foremost apprehension in cloud computing is trust and security. Trust is one of the serious complications for the acceptance and development of cloud computing [46].

(a) **Trustor and trustee:** the cloud is proceeding on the idea of trustee and trustee to set up trusting dealings. The variations that on-line accepted as true, with the distribution of characters will lessen the cloud service issues. The trustee, the cloud supplier consumer and related person existence the trustor [46].

(b) **Vulnerability:** The component of vulnerabilities enterprises aspect in cloud computing are uncountable. They influence from unintentional loss of privacy and data burglary to damage of stand-up and consequently currency [46].

(c) **Produced actions:** Customer's trust in cloud facility benefactors can produce a remarkable combination of anticipated movements. Enterprise surprises by means of cloud service and segments provide private and valuable data with the cloud computing provider [50].

(d) **Subjective matter:** Trust in cloud computing and technology is essential and particular as its online complement [47].

2.8.2. Trust Classification

- **Infrastructure trust:** Cloud service workers should deliver a secure organization, corresponding terminals, local area networks, and local servers. This can be appliable by means of security procedures also additional defensive trials to defend the organization [51].

- **Delegation:** A cloud service benefactor may possibly arrange an alternative cloud entity to receipts choices taking place on behalf of esteem. It will ehelpful to reserve allocation and services actuality [55].

- **Entity certification:** A third party propose guarantee toward a cloud entity and centered proceeding this entity's dependability [51].

- **Entity resources:** A Cloud service consumer imagines that a cloud service provider practices a characteristic that possesses his specific regulator [54].

- **Service Provision**: Cloud customer imagines cloud service companies to provide a provider to get admission to cloud carrier client sources. In detail, certain web programs download applets and cookies, to cloud service customers' resources [51].

2.9. Trust Management Techniques

Trust management techniques are divided into five groups; policy-based trust, recommendation-based trust, reputation-based trust, prediction-based trust and cryptographic [46].

- **Cryptographic** cloud arranges charity toward improving security in the cloud computing environment. It offers strong cryptographic nature to get admission is to manipulate mechanisms. The idea of the cryptographic cloud is that the records of manage and maintain the data by the consumer while protection of information is derived from cryptography. To guard records in the cloud numerous techniques have been used. This can get an addition to the manipulating method which incorporates verification and authorization. But these are usually disposed to defend records. Some others can use cryptography and make use of encrypted records. It offers a better solution for shielding records. Several encryption technique and algorithms has been used[50].

- **Policy-Based:** Trust is assessed by means of establishing policies, authorization and postulating a minimum trust to approve the admittance. The trust inceptions are increased from the trust effects or identifications. Results created on trust threshold is attained through observing and checking methodology (that uses the service level agreement) [54].

- **Recommendation-based Trust management:** Commencing end to end preceding an understanding of some individual’s trust events, they may direct their opinions as a curious entity. Tips unique forms, either detailed guidance or

transitive advice. Although a cloud provider consumer in a straight line mentions to attached by trustful dealings, that is well-known as definite advice[54].

- **Reputation-Based Trust Management:** Trust is calculated totally on accumulated estimation network in the direction of an individual. An entity with high popularity is generally dependent on several further entities. An improvement of this version is that the data charity for trust evaluation is collected from many distinctive entities at numerous conditions. This agreement much broader opinion approximately on cloud service company overall presentation[57].

- **Prediction-Based Trust Management:** For this method trusts mostly upon resemblance toward skills and pursuits among two entities. Consequently, these additions take as true with every difference in the event that makes have comparable views [56].

2.10. Related Work

This chapter involves the work done by the various researchers several modifications were introduced in AES in order to enhance the performance, speed and security by introducing some complexities in algorithms. These modifications are implemented on different software and hardware designs. However, preview framework security is always a concern due to some security constraints and problems with cloud computing. The security is provided to the information which is stored on the cloud by using cryptography algorithms. There are extensive security frameworks for cloud computing that uses enormous encryption techniques. This section consists of present related work about the cloud computing security, privacy, trust and the other presents related work to the available lightweight cryptographic systems. Out of these, a few of them are presented here.

2.10.1. Work Related to Cloud Computing Security and trust

So many researchers have dealt with the problem of cloud computing security, however, the most recent and related papers will be mentioned to this study here, as follows:

This paper focuses on the computation of different methods which explain how to increase data security so that prevention from different security attacks and breaches can be made. Mitigation approaches used in this research on the HMAC (Hashed Message Authentication Code) were ECC and MD5. This proposed solution is based on different security levels; as a result, access control, authentication, confidentiality, integrity, and encryption are achieved in this work. The authors performed and checked the security solution in real-time as well as in real cloud computing environment and also concluded that the solution that is been provided has very low overhead for upload and download service time [3]. This paper described the CloudSim simulator counting its architecture, aces, convicts, and CloudSim forms. Likewise, it characterized exactly how to practice CloudSim demonstration and replication in the cloud environment. Furthermore, it also describes the way to calculate approximate presentation limits like regular reversal time, amount, implementation period, types pan and entire conclusion period, etc. [58].

This paper reported dissimilar data safety and privacy security concerns in a cloud calculating environment and suggested a technique for dissimilar security services such as verification, approval, and privacy along with observing in suspension. Cloud computing plans a different technique for obtaining cloud data in the actual environment. 128 bit AES encryption is recycled for privacy, genuineness, and contact controller [59]. In the future work, load balancer by means of My Load Balancer optimization method has been compared with the two greatest well-known weight balancer techniques, i.e., Round-Robin and Supper Present Implementation Freight, also recognized as Active Monitoring Load Balancer. All such Java-based virtual techniques are used to create Cloud analyst toolkit. Graph procedures have been recycling to prove the comparative analysis [60]. The proposed solution will be able to provide the quality of service to the user of the cloud computing technologies. The functionality of User Behavior Analysis and profiling can be integrated in the solution developed for the Security Framework for Private and Public Clouds. In this paper discussed that there are many organizations which demands efficient solutions to store large amount of data efficiently. They discussed that cloud computing provides very scalable resources and different economic benefits for the reduction of operational costs. They discussed different key challenges which includes multi-tenancy, loss of control and trust. they categorized the research according to the cloud reference

architecture resource control physical resource and clod service management. They also discussed several security challenges that are elevated by existing or upcoming privacy legislation [61].

In past research, it was, evaluated how trust, security and shelter issues occur in the setting of distributed computing also enjoin courses that predominance which they'll appear as tended to it has the collaboration of diminishing expense by figuring and competence material goods, thick by means of on-request provision instrument anticipating a reimbursement for all deployment preparation of achievement. This makes consistency with laws connected to hold back and taking care of which is effortful to fulfil [50]. Researchers have endorsed a reliable idea that no longer simplest identifies deceptive consider feedbacks from agreement attacks but further more distinguishes Sybil attack son problem person's attacks proceeds apartment in preference or rapid term of time (i.e., tactful or infrequent attacks correspondingly). We and advance inaccessibility finding that preserve the trust regulator service at a relevant grade. We've acquired quietly an upraised quantity of consumers accepts by way of true with responses assumed on real-global smoke services to estimate our wished-for strategies [46].

Researcher have endorsed a unique framework, SelCSP, which enables the choice of the straightforward and equipped service provider. The framework estimates trustworthiness in phrases of context-precise, energetic believes and popularity responses. It furthermore figures out the ability of a provider is a concern in conditions of clearness of SALS in cooperation objects that is mutual to version interaction hazard and proposes an approximant of threat intensity elaboration in a contact. Such an approximation allows a customer to make choices concerning to choose a service supplier for a specified set of the interface [62]. In this research, suggest a conclusion management framework to achieve the gap amongst the need for inference and evaluation of mistrust result in cloud computing systems. Essentially, we offer a technique for cloud dealers or executives to evaluate the hypothesis of knobs for once. Similarly, it delivers cloud vendors a steerage sighted dynamically assigning encouragement [57]. This work offering an innovative assumption version known as ARICA establishment which maintains less confidence in the supposition importance of earner after more third-celebration feedback. Consecutively, the

ARICA version will increase the assumption on the consumer and will be helpful. Moreover, the anticipated model is based on five characteristics: accessibility, reliability, truthfulness, confidentiality and confirmation. This permitted launch has enough money for the assessment of the future ARICA trust model with two current schemes. Consequences show that the planned version provides a souled active exclusive impression [7].

2.10.2. Work Related to Cryptographic Systems

The complexity detects were an effect of dismiss logical purposes in the MixColumn conversion of AES. These reasonable tasks were eradicating in the modified version of AES. Afterward, on utilizing the modified AES, a 13.6% reduction in LUTs, 10.93% share discount, and a 1.19% reduction in interruption eating was attained. Likewise, the small dispersal rate met through the conservative AES at the initial nonentity, and important agenda sequences are spoken in [63].

In this research, they examined five metrics specifically: the graphic study, file size, radiance histogram, assessment by pixel, and show distance. In the file scopes, there were differences wherever it displays the regular worth of the fraction variations to −23.85% from the unique to the encrypt duplicate and −1.45% percentage worth from the innovative to the decrypt duplicate [64]. The modified AES contained 10 series for encrypting, and the replacement and addition processes of the columns have been substituted by the line change and pixel standard summary. These processes not only decrease the spell complication of the algorithm but also improve the dispersal aptitude to the CCAES (combining the chaos and AES) algorithm. The encrypted descriptions by the CCAES algorithm remained unaffected to the variance occurrences. The project algorithm is protected alongside the entropy occurrences. The simulation consequences illuminate that the minor deviations in the unique appearance and consequences in the important fluctuations in the encrypt duplicate and the innovative appearance cannot be retrieved [68]. The procedure of cryptography involves two main methods which are encryption and decryption. In the encryption method, a basic manuscript is converted to an innovative text which the others cannot deliver and understand additional than the receiver. Blowfish and AES procedures are exploited for executing a hybrid approach connected to cryptography.

This consequence in a cryptograph text which can merely be decrypted by the receiver this one [66]. In this paper, obtainable low-control AES architecture by exploiting humble shift catalogues and variation for key/data stored to decrease journey magnitude and control consumption. A low-power method, called clock gating is used to control exchangeable on S-box [67]. In the present study, Abikoye et al.'s modified AES algorithm [20] is presented which is also used in applications to make a comparison. K-L Tsai et al. presented the modified AES-based algorithm for power reduction in IoT using cloud computing applications [21]. In this paper, similarly, VM (virtual machine) allocation policy is used for security which is almost similar to the technique used in the previous work [68].

Describe the paper that cryptography plays a very important role for the security of data in cloud. They compared different cryptography techniques on the basis of encryption time" decryption time, key generation time and the size of file. They resulted that the symmetric algorithms are inexpensive as compared to asymmetric algorithms. They explained that the time of key generation is dependent on the size of key. They further suggested that in future we can elaborate schemes of asymmetric and symmetric algorithms and can extends the result on performance analysis [69].

2.10.3. Work Related to Security Framework Systems

The security framework is based on the multicloud environment to store digital data at all. In order to prevent data disclosure, they practiced a segmentation approach to fragment the input appearance into several areas. The integrity of the outsourced clients' data helps to verify watermarking technique. Any accidental change to outsourced clients' data can be detected by the digital signature and watermarking methods [70]. The framework presented in this study is more secure, and it provides more privacy to the data. This framework splits data into different blocks of bit. On every two blocks of bits, genetic algorithm is applied. Concluding output of each genomic algorithm procedure is a ciphertext along with two blocks of bits. Each ciphertext is stored on the cloud at a distinct location, and the location of the ciphertext is not secure. What makes it more secure from attackers to find the exact location of the ciphertext? The innovative security framework puts on a genetic algorithm on minor block size that increases the security. Furthermore, the framework uses the proficiency list aiming to secure and to access data [24].

In this paper, authors proposed a new framework that ensures the data security and integrity and also focused on the encryption and decryption approaches facilitating the cloud user with data security assurance. The proposed solution talked about the increased security along with the performance. Their solution has also included functioning of the forensic virtual machine, malware detection, and real-time monitoring of the system [71]. In this paper, the authors suggested a framework such that the objective is to store data in various clouds. The given framework is found based on 3DES and RSA encryption. On the contrary, this methodology is lacking in efficiency, privacy, and overload middleware through multiple functions [72]. In this paper, the authors studied, multilevel licensing framework approval preservation cloud penetrating data. Safeguarding the familiar and delicate cloud data is obtainable by the three covers' framework. Those restrictions are being the security and privacy strategies, safety and approval policies which outcomes from the three films' security framework [25]. In this paper, the authors proposed quality metrics and details probe on instance cloud service broker frameworks are provided. These streak metrics help in enforcing standards on cloud service providers by using quality-based cloud service broker framework (QCSB). The algorithm and implementation of QCSB have been obsessing. At last, the authors concluded that the proposed material QCSB not only assists cloud computing to locate optimal CSP (cloud service provider) for cloud services but also affiliates candidate CSPs according to user quality preferences [26].

This paper showed an overview of the latest research studies that are going on in fog computing and the IoT and its uses; it also enlightened the research gaps and directions for further future research studies in the integration of fog computing and IoT (Internet of Things). A modern fog computing framework was presented [73]. Therefore, this paper put forward in overcome the gap in classifying all conceivable issues that interrupts the confidentiality of cloud customers and propose a theoretical framework clearance of sound effects. The chief objective of this paper is to classify the influences that might affect separate user's privacy. We suppose our learning to classify impending privacy matters which develop extra important to cloud users [74]. This paper suggests a security framework contains of three chief services for security, important and storing. Security is provided as a facility to users. This framework contains of two security services for dissimilar kinds of data. Users have to indicate slightly one security service founded on

their optimal. Key generation is additional service in the framework which delivers crucial for security service by the means of sending the key in a straight line to the users. Keys used for security service are not well-known to additional cloud service in the framework. The framework defends occurrences from classified and external the cloud. It increases the security in the public cloud atmosphere [12]. In general, the main purpose of all research studies related to the subject areas is to examine the imaginable conducts to advance the security of cloud computing services. Thus, in this effort, a secure framework has been planned for securing intimate chores existence kept in cloud systems by means of AES encryption approaches. Finally, a comparison of the results obtained through this proposed framework and traditional framework work formulated in the past is made which showed significant improvement of cloud computing using the proposed framework. The differences between our modified AES and previously developed or modified AES in the JAVA cipher-based security framework have been discussed in this manuscript. It is pertinent to mention here that our trust-based framework blocks the suspicious users from the network and maintains a queue for such users to protect the trusted users.

2.10.4. Details of Data Security Model of Literature Survey Papers

In the following table showing some details of recently published papers from the 2015 to 2020. With their major issues benefits and limitations that is been observed in this thesis.

Table 2.1:Summary of data security models papers

Ref no.	Techniques	Issues	Benefits	Limitations
[75]	Cryptography, steganography	To handle security issues	Providing image data security	Algorithms are not robust and poor data hiding capacity
[76]	HMAC, RSA, AES	Design a secure framework	Indexing makes searching easy and study of various cryptography tech that give better execution of time.	Algo not proven mathematically and Time complexity
[77]	Cryptography, steganography	Steganography Secure migration of data	Provides multilayered protection to data, Less costly app.	Poor Implementation and Comparisons with other pproaches not included

[78]	AES	Network integrity	Fast, flexible, secured mechanism Support all types of data (text, audio, video, etc),	Too many keys to distinguish.
[79]	vector commitment, Asymmetric Group Key Agreement, verifier-local revocation group signature.	Efficient public integrity verification with secure group client repudiation.	Secure against the collusion attack.	More computation cost.
[44]	Secure and Scalable Data Collaboration service (SECO) scheme.	Protected and adaptable information collaboration assistance in distributed computing	Secure against ciphertext attacks	Data consistency is not achieved.
[80]	Identity privacy-preserving public auditing protocol	Efficient chameleon hashing-based privacy-preserving auditing	Identity privacy preserved, low computation cost.	The cloud server has large computation cost.
[81]	Key generation (KeyGen), Proof, Verify, Revoke member phase.	Public verification for shared information in distributed storage.	Data privacy is achieved.	The high computational burden on the batch administrator.
[82]	Public auditing and dynamic data update scheme.	Public Auditing and Data Dynamics for Data Storage Security	Resistant to replace, replay and forge attacks.	More computation cost on the client-side.
[83]	Deduplication scheme for encrypted data.	Protected information deduplication with active ownership administration in the cloud repository	Prevents data leakage, assures information truthfulness.	Incurs additional computational overhead.
[84]	Threshold Data Deduplication Scheme.	Secure Threshold Data Deduplication for Cloud Storage.	Prevents deduplication of unpopular data.	Low space-saving efficiency.
[85]	Flexible and verifiable search scheme, Verifiable search scheme for multiuser.	Verifiable search for outsourced database.	Supports efficient data update, cost-efficient.	More computation overhead at the client-side.

[86]	Genetic algorithm heuristic method	Field of cloud computing, trust is the major issue	The adaptive evolution process of natural systems are imitated by GA which is stochastic optimization search procedures	Under contemplation is security and privacy problems
[87]	RSA-based CP-ABE scheme with constant size key and cipher text.	Offer attribute based lightweight encryption scheme with AND Gate	Efficient and fast as compared to bilinear map based ABE scheme.	If adversary somehow succeeded to derive the key Km from available public information, then he/she can succeed in retrieving the plaintext message.
[88]	IoT Agent based security mechanism	To isolate IoT function from the device and implement it on the cloud environment.	It uses IoT virtual clones which reduce the computation task physical IoT device.	As virtual clones are always online &have all replicated data from the physical device, so there is a risk of revealing the privacy of information.
[89]	End-to-end IOT Security middleware for cloud-fog communication	To provide end-to-end security mechanism for cloud-fog communication.	It offers flexible security configuration. Less expensive	For higher security requirements key has to be generated using RSA or Diffie-Hellman which are quite computation intensive.
[90]	ABE and ABS based secure data access control with a cipher text update	Secure data access control scheme for fog computing.	Significantly reduces the Computation work of IoT device.	Computation intensive as it is based on bilinear maps. Fog nodes are not fully trusted.
[91]	RFID based mutual authentication protocol	Cloud based Lightweight mutual authentication for RFID systems.	Its uses one-way hash and time stamps to ensure the update of information and synchronization attacks.	Scalability. Key allocation for mobile/stationary users in real time.

[92]	Biometric-based user authentication scheme	To add biometric credential along with password and smart card credentials to Authentication mechanism.	Multifactor authentication with a high level of security	Uses an open channel for Communication Memory requirements cannot be predicted for real-time environment in advance.
[93]	CoAP and DTLS based secure communication architecture for IoT devices	To incorporate DTLS-protected secure CoAP protocol for IoT devices and cloud-based host.	Suitable for IoT protocols	DTLS handshake is challenging due to public-key cryptography. Varied memory requirements.
[03]	HMAC (Hashed message authentication code), ECC and MD5	Configuration, storage, sharing are all possible in the cloud environment.	Security establishment based on access control, authentication, confidentiality, integrity and encryption is Achieved	Very low overhead has been observed for upload and downloads service time.
[94]	ABE	Efficient and generic construction of ABE	Instantiation of ABE with verifiable outsourced decryption is more efficient than the existing scheme.	High bandwidth utilization and cost doubling problem
[95]	Ethereum blockchain and (ABE)	Design framework decentralized storage system interplanetary file system.	Decentralized storage systems and propose a framework that combines the decentralized storage system.	Providing wrong result in traditional cloud.
[96]	Homomorphic Encryption (FHE)	Handling termination by message passing between server and client	FHE provides the capability of performing computations over encrypted data	Challenged facing like loop handling, data structure and decision making.
[97]	Encrypted Bloom filters	Cloud service user to detect unauthorized modifications to his outsourced data	Minimize storage and network overhead depending on the database structure and workload	Overhead network burden, storage problem due to workload

[98]	Advanced Encryption Standard (AES), MAES	The energy issue is now becoming the prime concern	Modified version of AES for Resource-Constraint Environments.	S-Box and Mix Columns are the most energy consuming stages in encryption and decryption
[99]	OTP Remote authentication biometric data	Improve authentication in the cloud	Improve the user identification process, which uses a common biometric recognition system	Still security problem, persists, data was illegally disclosed.
[19]	Advanced Encryption Standard (AES)	Improve the security strength	Tried to solve the problem by incorporating the changes in key expansion module.	The fault injection attacks that could be used to reveal AES key
[100]	Fine grit inspection mechanism	Access control model which is time controlled and fine-grit	Effectively solve the changeable tenants and flexible resource distribution in cloud computing.	Time restrained and fine grit mechanism only.
[63]	AES	Modified (AES) improved diffusion and confusion properties and the ciphertext	Modified AES can be successfully decrypted and recover back the original plaintext. Improvements were noted in the confusion property, still room for improvements.	Worked on AES key scheduling to increase diffusion and confusion rate and enhance the security of AES.
[68]	SC-PSSF (Previous-Selected-Server-First, PSSF)	To solve the security problems about VM co-residency,	Reduce the total energy consumption of hosts while load balancing deserves better works to improve VM allocation policy.	If the previous server is overloaded with tasks then this algorithm may not give efficient results.
[101]	Review Paper trusted computing and cryptography	Discuss the security issues of data storage.	Issues related to data location, data recovery, security, availability and integrity.	To increasing the security of the information sent, it can also minimize the key distribution between the two parties.

[9]	Compared RSA with ElGamal and Paillier	Design of framework for sharing a file to ensure security	Proposed the framework to share a file in a secure manner using public key infrastructure, store, share, and download by ensuring and satisfy.	Data transfer security needs and the threats involved
[20]	Advanced Encryption Standard (AES symmetric cryptographic techniques	An enhanced AES algorithm that was achieved by modifying its SubBytes and ShiftRows transformations	The modified algorithm is evaluated in terms of avalanche effect and modified AES achieved to increase in the execution time	Several security techniques have been proposed towards preventing data and information from unauthorized attacks.
[24]	RSA algorithm	Design framework of security to ensure Cloud Data Storage	Framework for ensure the security of Cloud Data Storage(CDS).	Agent-based security framework for via a trust model, encryption method, and integrity technique to increase Cloud performance.
[102]	Elliptic curve cryptography	Design framework cloud-based efficient authentication	ECC-based suitable framework for smart medical system in cloud environment.	Cloud is not fully safe in the networking system, so an authenticated framework required to maintain the security and privacy.
[103]	Elliptic curve cryptography.	Among these some protocols have security issues	Real-life application in Smart grid communication.	Cloud is not fully secure. security issues like patent anonymity and unlink ability, doctor anonymity and unlink ability, data confidentiality, integrity, etc
[104]	Cryptographic techniques such as, symmetric key en/decryption TS and hash function	Provides a scalable platform to support intelligent transport systems	Improving traffic management, street security, and traveler guidance	Not secure against patient anonymity

2.11. Summary

- Although cloud computing is giving several benefits that includes return on investment, increased performance and security of the cloud architecture. Customer data with growing security threats, challenges and issues. On the other hand, this technology facing variation of matters and challenges wherever the privacy and security issues can be measured as the greatest challenging.

- Cloud computing security in general was reviewed, analyzed and summarized, using different cryptography systems of encryption, and comparisons are made in terms the advantages, disadvantages and goals of these methods.

- Security methods were mentioned to improve the protection of data stored on cloud computing environment. Secure Framework which are designed for both hardware and software were reviewed, and comparisons were made in terms of structures, key lengths, and number of rounds.

- A detail discussion on the existing designed and developed techniques which has been providing the security to the cloud computing and other computing networks.

- In the following chapter the Security Architecture will discuss that include security implemented in real time system. Also, different perspectives of the development technique designs of the Security Framework along with its implementation has been presented.

CHAPTER 3

SECURE FRAMEWORK ENHANCING AES ALGORITHM IN CLOUD COMPUTING

3.1. Overview

The chapter discusses the development and designed of security framework which has been to evaluate security controls and mechanism execution on each layer of the cloud model. It always be a big challenge during research to design a conceptual framework. That framework covers and fulfil all the objectives of the research and it designed in such a manner that it can perform all the activities and tasks which are required in our research. Increasing the speed of the encryption and decryption algorithm, while keeping the security level high is a vital for a lot of applications, this target require high security level with limited resources. The AES algorithm explained in this chapter put light on consumption of unnecessary time to achieve the necessary complexity for the purpose to meet the security level.

3.2. Architecture of the Proposed Secure Framework for Cloud Computing (SFCC)

The architecture of the proposed Secure Framework for Cloud Computing (SFCC) is presented below in Figure 3.1.

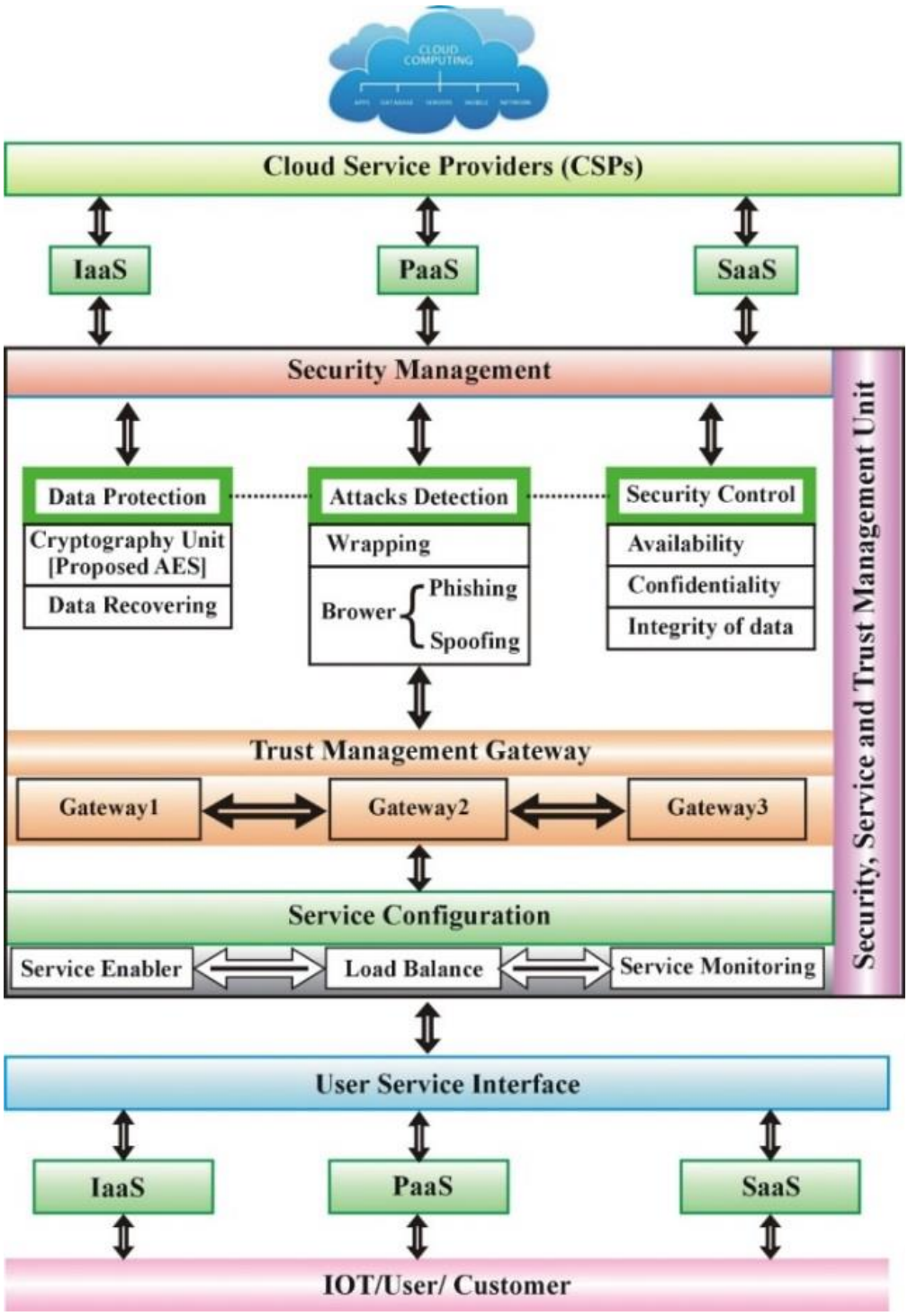

Figure 3.1:Secure Framework for Cloud Computing (SFCC)

Framework of secure cloud computing is proposed on the security architecture shown in Figure 3.1, which describes the information for each component and their applications which are required for secure technologies to operate between components in cloud computing. This framework acts in the following conditions checking security, privacy, load balancing, and trust. When the user directs a demand to the cloud

benefactor, it responds to the user's request and passes the data through framework gateways. The proposed framework includes the following components:

3.2.1. **Cloud service provider (CSP) layer:** the CSP controls the important sources and ability in construction and calculates the dispersed cloud storage servers' processes and directs the live obscure work out method. Its main component is **software as a service (SaaS);** this is a model in which end users are provided software application (as a service). **Platform as a service (PaaS):** this model proposed an atmosphere for requests. Development tools that are essential for advanced applications are also provided in this model. **Infrastructure as a service (IaaS):** this is a platform that offers compulsory properties such as physical machines, virtual machines, and virtual storage.

3.2.2. **Security service trust management unit:** security service trust management controls all the units which include security management; trust management gateways also control the service configuration, respectively. Further details of all units are described in the following.

3.2.2.1. **Security management layer:** the security management factor offers security and privacy details and implementation functionality. Security service has the following modules and their details.

Security control unit: availability is the percentage of time a customer can access the service. **Confidentiality** (authentication, authorization, and identification) is an integral component of security. It ensures that the information stored on the cloud is protected against the unintended or unauthorized access. **Identification** user is typically skillful by retaining usernames and passwords after utilizing web browser in order to admit in Cloud. **Integrity of data** security control is responsible for maintaining the accuracy of data computation that is coming from the combination of different files and is also responsible for its delivery.

3.2.2.2. **Attack detection unit:** ultimately, slightly usual activities that hover the cloud security necessities (e.g., integrity, confidentiality, and availability) are measured to be occurrences. **Wrapping** is when the

attacker attacks by wrapping the communication between two people, while the users do not know this and think data are still coming from the actual root. Unethical **browsing** is to find bad actions happening, for example, **phishing and spoofing** and changing browser certificates.

3.2.2.3. **Data protection unit:** proposes the AES algorithm to enhance the data security by means of cryptography techniques using AES ciphers as they can encrypt 128 bits' data blocks within 1000 blocks per second with the double round key feature with less power consumption, load balancing, trust, and resource management on the network efficiently. We have used symmetric identification for security, i.e., the same key for encryption and the same key for decryption as identification of data streams in the form of security. It provides greater efficiency for software as well as hardware. The advantage of using symmetric key is to secure a large amount of data. **Data recovery:** if data is lost in a disaster that it has a capability to regain it or restore it.

3.2.3. **Trust management gateway layer:** for the fourth layer, trusted gateways are implemented. These gateways get the encrypted data and decrypt only if the trusted source is connected with a valid internet protocol address of a given domain. These gateways support the issues of trust. There are three gateways in which two are in an alternative manner. In case of the normal gateway is being attacked and misused, other safe gateways shall be chosen to ensure data communication.

3.2.4. **Service configuration layer:** the service enabler makes provision for personalized cloud service using the user's profile for integration and interoperation. **Load balancing** can be implemented on hardware, software, or a combination of both. It is important in this configuration that all instances of identity server share the same directory server. **Service monitoring:** an automatic facility-checking system to assure an extraordinary level of facility presentation and obtain ability.

3.2.5. **User service interface layer:** this layer provides different services to select the user via the internet: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS).

3.2.6. **Service configuration layer:** the last unit for the user, IOT, and customer to send and receive data.

3.3. Introduction to AES Algorithm

Advanced Encryption Standard (AES) also popular as Rijndael algorithm. It is also known as symmetric block cipher. It is known that DES was not secure as because of advancement in computer processing power. It only encrypts data blocks of 128 bits using symmetric keys 128, 192, or 256. It also has variable length of key 128, 192, or 256 bits; by default, use 256. It encrypts the data blocks of 128 bits in 10, 12 and 14 round dependent on the key size. AES encryption is precise firm and flexible. It can be executed on different platforms particularly organized in small procedures. AES has been verified for numerous security applications [105].

Every round of AES is established by following transformations according by [106].

- AES conclude 128-bit of data block, which described the data blocks, has 16 bytes. In all sub-byte transformation of, every bite 8-bit chargeable box which is known as Rijndael Sbox. The figure 3.2 shows an example for a subbytes process.

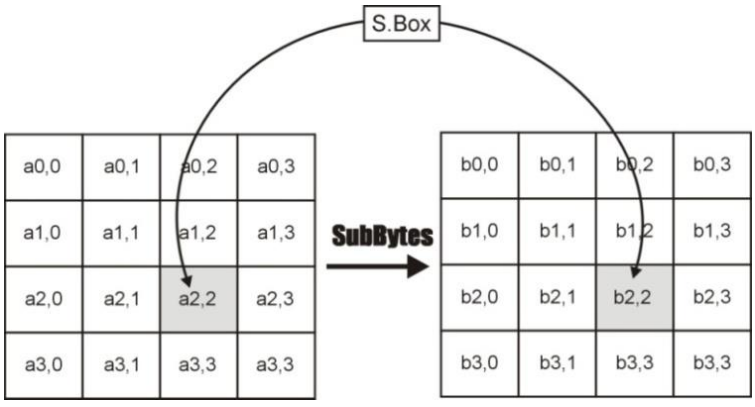

Figure 3.2:SubBytes Step applies in bytes.

- It is very ordinary byte transformation, the last three rows bytes of the state, depending upon the row location, of row, is shifting cyclically. For second Row1-byte circular is performed left shift, for 3rd and 4 row 2-byte and 3byte

left circular left shift are performed respectively. The figure 3.3 shows an example for a ShiftRows step.

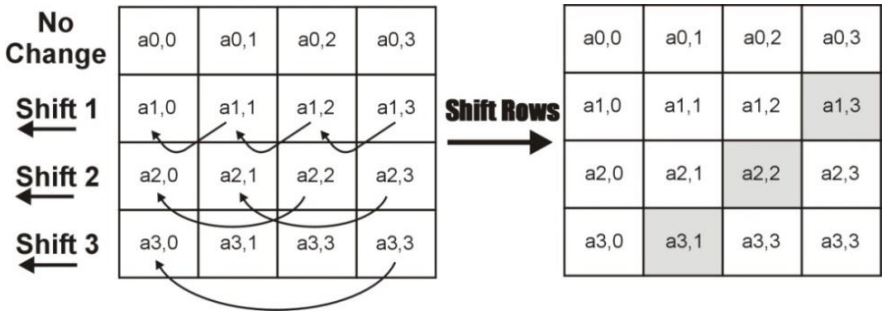

Figure 3.3:ShiftRows example for encryption.

- This round is approximately equivalent to matrix multiplication of each Column of the states. Fix matrix is multiplied to each column vector. In all operation bytes are taken as polynomials instead of numbers. The figure 3.4 shows an example for a Mixedcolumns process.

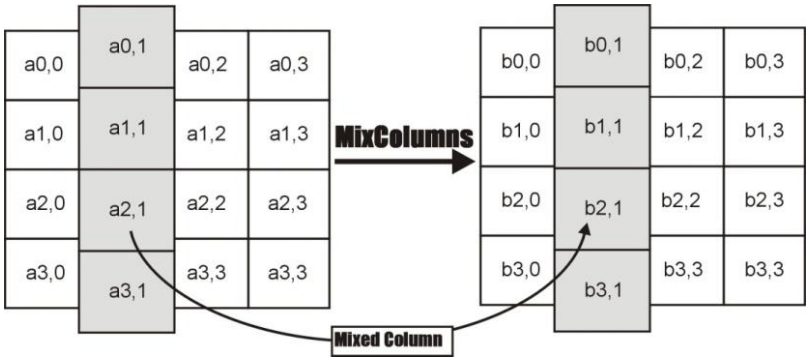

Figure 3.4:MixColumns process.

- It is a bitwise XOR between the 128 bits of present state and 128 bits of the round key. This is inverse transformation is its own. The key addition process is shown in Figure (3.5)

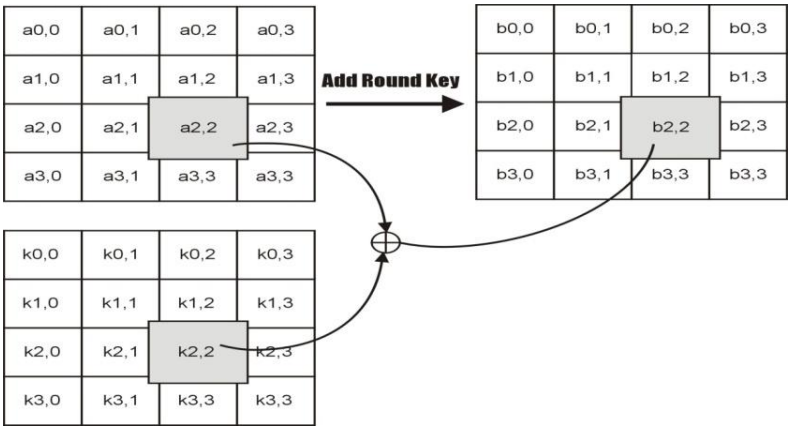

Figure 3.5:Key addition process.

3.4. Algorithm

Alogrithm 1: To perform an Enceyption

Input: Plain text

Result: **Encryption**

Get cipher text;

while ***Mixing Rows and Columns*** do

    Compute Password and Values;

    if ***Password*** then

        Compute Time;

        Add Double Round Key;

    else

        Add sub Rows and Columns;

    end

end

Alogrithm 2: To Perform a Dceryption

Output: Cypertext

Result: **Decryption**

Get cipher text;

while **Original plain text** do

    Get encrypted cipher text;

    if ***Total length*** then

        Split ino original table;

        Remove Double Round Key;

    else

        Remove Rows and Columns;

    end

end

Algorithm is written in two parts. The first part describes the encryption process and the second part describes the decryption part. We followed the pattern mentioned in base paper and other papers which is standard format.

Input: Cipher Text

Output: Encryption/Decryption

3.4.1. Changes in Traditional AES Algorithm

The high-level flow of the proposed AES algorithm in a standard way is presented in Figure 3.6.

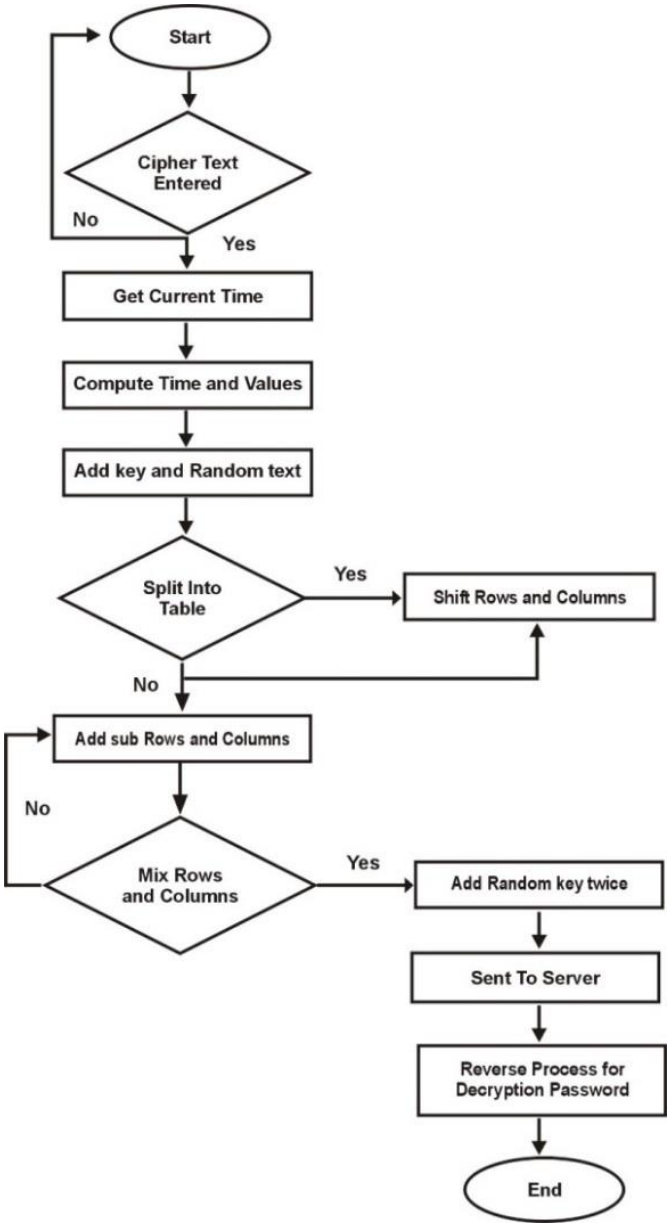

Figure 3.6:Flow diagram proposed algorithm

3.4.2. Changes in the Traditional AES Algorithm vs. the Proposed Algorithm

The cloud computing confidentiality framework is presented in this paper. In this framework, data integrity mechanism is used to enhance the data security by the means of cryptography technique. The modified AES (advance encryption standard) ciphers as it can encrypt 128-bit data blocks within 1000 cycles with low power, time, and delay of network consumption. The other work of the frameworks is load balancing, trust, and resource management on the network efficiently.

We have used symmetric identification for security, i.e., the same key for encryption and decryption as identification of data streams in the form of security. The difference between the proposed and previously developed AES is that we have encrypted 1000 blocks per second with the double round key feature. Previously developed AES uses a single round key with 800 blocks per second. The advantage of using symmetric key is to secure a large amount of data.

3.5. Experimental Setup and Implementation of SFCC

The SFCC can be implemented in real time. The results gathered from the simulations are very accurate. These results are theoretically consistent. Everything is implemented accordingly. Codes are very consistent with real-time mechanisms. The SFCC is developed using CloudSim [107] and iFogSim simulators on the Eclipse integrated development environment. CloudSim is a very well-known and popular among simulators [108] for cloud-based applications. It is responsible for the simulation and events handling at cloud. Some libraries are used for different purposes. Libraries used are JavaScript object notation (Json) data saver, common math, and JFreeChart.

The developed simulation comprises SFCC. The proposed framework is generic so that anyone could put one's idea or logic in this simulation and get the required results. It helps the user to test different scenarios under the proposed algorithm. The simulation has the ability to store and generate a large amount of data. It allows a user to measure the factors such as encryption, description, power consumption, network usage, delays, trusted devices, and service management. The advanced encryption standard for encryption and decryption for data protection is used. The comparison of the algorithm with the previous unmodified algorithms is discussed in later sections. The characteristics of the layers and devices are described in Tables (3.1–3.11).

3.5.1. Components

Data Centre refers to principle hardware, while the cloud refers to off-principle of computing. The cloud stores your data in the public cloud, while a data centre stores your data on your hardware. Data centre configuration is displayed in Table 3.1.

Table 3.1:*Data Centre Characteristics Cloud*

Name of device	Cloud
Level	1
Uploading Bandwidth	5000 Gbits/Sec
Downloading Bandwidth	12000 Gbits/Sec
Million instructions per second	130.0 ms
Ram	45000 GB
Rate per processing usage /MIPS	100000

Infrastructure as a service (IaaS): this is a platform that offers compulsory resources such as physical machines, virtual machines, and virtual storage. Infrastructure-as-a-service configuration is displayed in Table 3.2.

Table 3.2:*Data Centre Characteristics of Infrastructure as a service*

Name of device	Cloud IAAS
Level	2
Uploading Bandwidth	4000 Gbits/Sec
Downloading Bandwidth	5000 Gbits/Sec
Million instructions per second	50000 ms
Ram	40000 GB
Rate per processing usage /MIPS	400.0

Software as a service (SaaS): this is a model in which end users are provided software applications (as a service). Software-as-a-service configuration is displayed in Table 3.3.

Table 3.3:Data Centre Characteristics of software as a service

Name of device	Cloud SAAS
Level	2
Uploading Bandwidth	4000 Gbits/Sec
Downloading Bandwidth	5000 Gbits/Sec
Million instructions per second	60000 ms
Ram	40000 GB
Rate per processing usage /MIPS	400.0

Platform as a service (PaaS): this model proposed an atmosphere for requests. Development and deployment tools that are essential to advance applications are also provided in this model. Platform-as-a-service configuration is displayed in Table 3.4.

Table 3.4:Data Centre Characteristics of platform as a service

Name of device	Cloud PAAS
Level	2
Uploading Bandwidth	4000 Gbits/Sec
Downloading Bandwidth	5000 Gbits/Sec
Million instructions per second	60000 ms
Ram	40000 GB
Rate per processing usage /MIPS	50000

Security management: the security management factor offers the security and privacy details and implementation functionality table. Security management configuration is displayed in Table 3.5.

Table 3.5:Data Centre Characteristics Security Management

Name of device	Security Management
Level	4
Uploading Bandwidth	5000 Gbits/Sec
Downloading Bandwidth	5000 Gbits/Sec
Million instructions per second	40000 ms
Ram	35000 GB
Rate per processing usage /MIPS	600.0

Gateway devices at the second-last level of the hierarchy gateway devices are created. These gateway devices are part of the layer responsible for communicating with proxy servers and cloud devices. Here are the characteristics of the gateway devices. Gateway device configuration is displayed in table 3.6, 3.7 and 3.8.

Table 3.6:Data Centre Characteristics of Gateway1

Name of device	Trusted gateway1
Level	3
Uploading Bandwidth	3000 Gbits/Sec
Downloading Bandwidth	4000 Gbits/Sec
Million instructions per second	30000 ms
Ram	20000 GB
Rate per processing usage /MIPS	1000.0

Table 3.7:Data Centre Characteristics of Gateway2

Name of device	Trusted gateway2
Level	3
Uploading Bandwidth	3000 Gbits/Sec
Downloading Bandwidth	4000 Gbits/Sec
Million instructions per second	30000 ms
Ram	30000 GB
Rate per processing usage /MIPS	400.0

Table 3.8:Data Centre Characteristics of Gateway3

Name of device	Trusted gateway3
Level	3
Uploading Bandwidth	4000 Gbits/Sec
Downloading Bandwidth	4000 Gbits/Sec
Million instructions per second	50000 ms
Ram	34000 GB
Rate per processing usage /MIPS	600.0

Service configuration: This facility modifies the cloud service using the user's profile by integrating service enabler, load balancing, and service monitoring. Service configuration is displayed in Table 3.9.

Table 3.9:Data Centre Characteristics of Service Configuration

Name of device	Service Configuration
Level	1
Uploading Bandwidth	5000 Gbits/Sec
Downloading Bandwidth	5000 Gbits/Sec
Million instructions per second	100000 ms
Ram	40000 GB
Rate per processing usage /MIPS	500.0

Service provider: this is the last unit for users and customers to send and receive data. Service provider configuration is displayed in Table 3.10.

Table 3.10:Data Centre Service Provider Characteristics

Name of device	Service Provider
Level	1
Uploading Bandwidth	5000 Gbits/Sec
Downloading Bandwidth	5000 Gbits/sec
Million instructions per second	50000 ms
Ram	20000 GB
Rate per processing usage /MIPS	100.0

Virtual machines are created and allocated to hosts to support processing and offloading the modules to support the load balancing mechanism. These virtual machines come with the proposed strong encryption algorithm to support the

security and trust feature. The virtual machine configuration is displayed in Table 3.11.

Table 3.11:Virtual Machine Configurations

Virtual machine Number Level	Virtual machine Number	Processing Elements	Bandwidth (Uplink)	Latency Input
Level 0	2	20000	800	10
Level 1	4	18000	1000	6
Level 2	6	16000	1200	8

The materials and methods section should contain satisfactory features to repeat all procedures. It may be divided into headed subsections if variety of methods are described.

3.5.2. Physical Topology of SFCC

The physical topology shows the pattern of nodes and devices in the network. Physical entities are shaped and specify competence, capability, and configurations. These entities include sensors, actuators, gateways, and cloud VM (virtual machines). The links between these entities and their configuration are also established. Physical network topology is important to understand the pattern of the network, how various network devices are organized, and how they interconnect with each other. These configurations and capacity determine the load a network can tolerate and the amount of data it can transfer. The physical topology is shown in Figure 3.7.

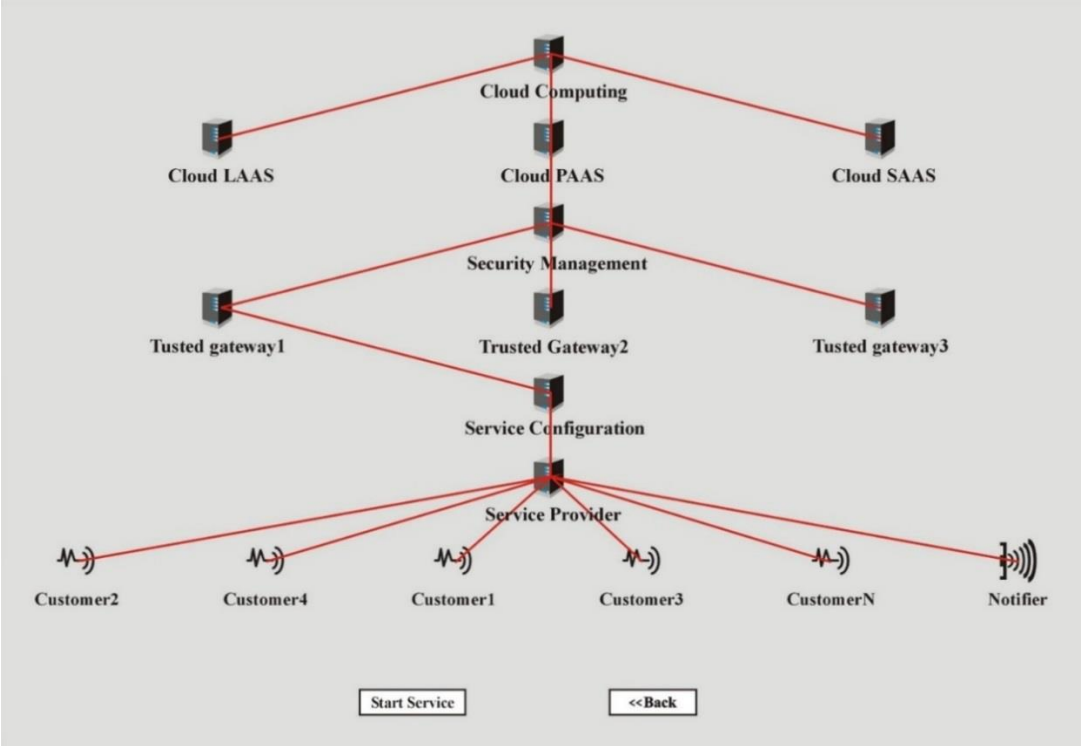

Figure 3.7: Proposed Network Topology of SFCC

The computing mechanism of cloud always happens at the top. Cloud stays at the top to manage the lower-level architecture [109]. The three different types of cloud stay below the top layer and act as CSPs [110] according to customers' need. For the third layer, the virtual machine allocation policy mechanism is implemented to support data offloading and privacy for security [111] in the proposed system. Offloading the modules not only provides load balancing but also solves the security issues of cloud by providing a new layer on the hosts. Virtual machines are created and allocated to the hosts to support processing and offloading of the modules to support the load balancing mechanism. These virtual machines come with a strong encryption algorithm to support the security and trust feature.

The Virtual machine requires some storage and processing capabilities similar to a host H in nature. Equation 1 represents the conditions for creating a Virtual machine. The Vm size is always smaller than the available host H and storage S where the number of Vms depends on the size of load ($\boldsymbol{\beta}$).

$$\text{If } \mathrm{H}=\{\mathrm{H1}, \mathrm{H2}, \mathrm{H3}, \ldots \mathrm{Hn}\} \text{ and } \mathrm{V}=\{\mathrm{Vm1}, \mathrm{Vm2}, \mathrm{Vm3}, \ldots \mathrm{Vm\ N}\} \text{ then}$$

$$\exists\, Vm \in H \cup S : Vm \propto \beta where H \cap S \gg Vm$$

$$: Vm1, Vm2, Vm3 \ldots Vm < H1, H2, H3 \ldots H \;\; \forall\, V \;\exists\; Vm1, Vm2\,, Vm \ldots VmN \in H \qquad (1)$$

Equation (1) represents how VM creation is carried out under various rules and conditions

For the fourth layer, trusted gateways are implemented. These gateways get the encrypted data and decrypt only if a trusted source is connected with a valid Internet protocol address of a given domain. These gateways support the issues of trust [112]. There are 3 gateways in which 2 are alternate manner. In case of a normal gateway is being attacked and misused, other safe gateways shall be chosen to ensure data communication, as shown in Figure 3.8.

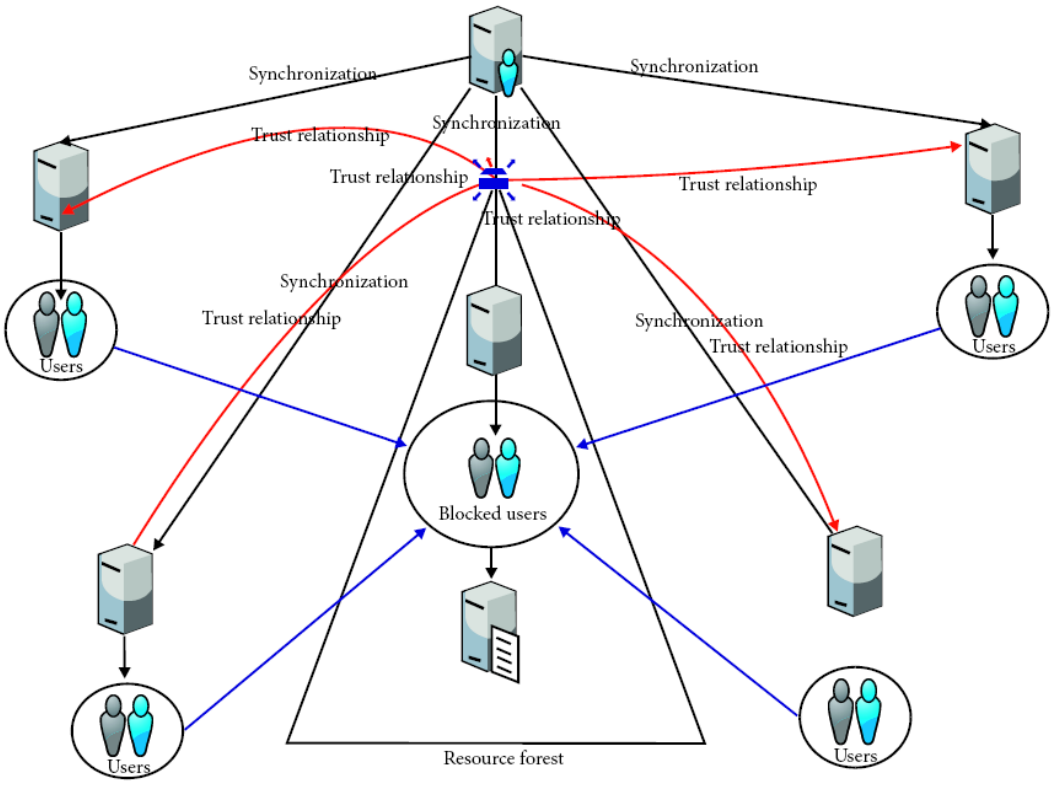

Figure 3.8:Trusted gateways

Trusted gateways put the blacklist users into the blocked users' category to ensure the security and privacy of trusted users. The fifth layer is responsible for 3 functions. These functions include service monitoring, load balancing, and service enabling/disabling. The bottom-most layer is based on the users of cloud, and it represents the Internet-of-Things layer in the proposed system. This is how all the aforementioned proposed frameworks work. The trusted customer stays as long as a mediator (trustee) stays. And a mediator stays as long as the cloud service providers are trustable. The chain of trust can be seen in Figure 3.9 [107].

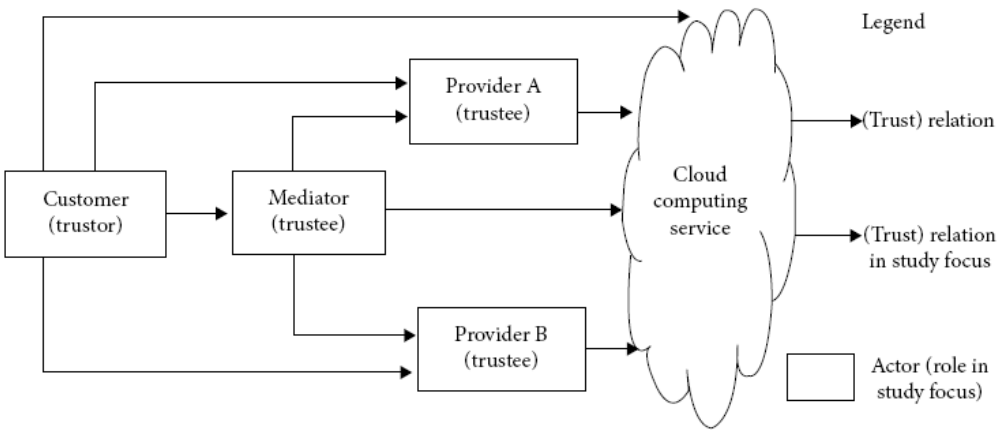

Figure 3.9:mediator of Cloud service providers trusted chain

3.5.3. AES Substitution Box (S-Box)

The primary stage to around, remains to organize a byte by byte replacement through a lookup table called a substitution box or simply S-box. The S-Boxes carry out one to one plotting for all byte values from 0 to 255 in 16×16 arrays. Replacement is a nonlinear conversion which achieves misperception of bits. A nonlinear revolution is vital for each current encryption algorithm and shown to be solid cryptographic original in contradiction to direct and disparity cryptanalysis. The S-box is shown Figure 6. All values are represented in hexadecimal notation [113]. The general substitution box for adding round keys is given in Figure 3.10.

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
	1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
	2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
	3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
	4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
	5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
	6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
	7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
	8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
	9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
	a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
	b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
	c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
	d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
	e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
	f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Figure 3.10:Substitution Box [113]

Rows are represented by x, and columns are represented by y. The mixing process is done with XOR denoted by the symbol $\oplus$. The binary example in the following will illustrate the functionality of the XOR operator. The row and column mixing and shifting are done by Shift (x_row, y_clolumn) function. The transformed arrays xand y are converted into binaries using ASCII__ASCII 256 standard. Then, the XOR operator performs its $\oplus$ operation on the bits to generate the ASCII-(American Standard Code for Information Interchange) generated ciphertext. The

cryptographic technique used in SFCC is presented in the low-level language as follows:

$$CiT(enc) = 1/N \sum_{i=0}^{1} X_r \oplus Y_c \quad (2)$$

$$CiT(dec) = N \sum_{i=0} X_c \oplus Y_r \quad (3)$$

→putfieldjavax.crypto.Cipher.spi :javax.crypto.CipherSpi

exec_0 [this] exec_2 [x__rows] (i)

→putfieldjavax.crypto.Cipher.provider :java.security.Provider

exec_0 [this] exec_3 [y__columns] (ii)

→putfieldjavax.crypto.Cipher.transformation :java.lang.String

exec_0 [this] (iii)

→getstaticjavax.crypto.CryptoAllPermission.INSTANCE:

javax.crypto.CryptoAllPermission (iv)

→putfieldjavax.crypto.Cipher.cryptoPerm :javax.crypto.CryptoPermission

exec_0 [this]aconst_null (v)

→putfieldjavax.crypto.Cipher.lock :java.lang.Object return ∏; (vi)

The example of ⊕ is given below.

Let X = 1110_2 and Y= 1001_2Then XOR of X and Yare represented by Z:

$$\boldsymbol{Z = X \oplus Y = 0111_2}$$

$Z = 0111_2$ is the result of this operand. Table 4.12 *below displays the result in tabular form.*

Table 3.12 XOR Operations

X	***Y***	***Z (Result)***
1	1	0
1	0	1
1	0	1
0	1	1

3.6. Case study will be explained below with visuals and texts

3.6.1. Scenario-1

It this case study the Service Provider (SP), End User (EU) guide about the information handing appliance of information handling formwork to enhance information Management. The sceneries of this study through customer mist contributed in cloud service by giving the information about his credit card to the cloud portal suppose the person (Pay-as you go) service use also consume the

hardware and service of new infrastructure service. The forcibility use given a new name (SaaS Software –as- service) or PaaS (Platform-as-Service). A presentation has been development for medical Appearance Processing (MEP) for the handling of medical pictures that created from the image taking machine. These picture will store on cloud computing data collecting Centre for further processing and issuing a find report. The provider who provide the service is ready for cognitive services for public cloud for the scenario that discuss above. The supplier service only concern when model requested responses use for line up a lot of appeals upcoming from the person that live different areas. Due to this facility close down and service supplier not able to control all request and able to provide suitable information to all requests. In additionally all the staff member, client, employee that employ in hospital or doctor not acquire the best possible result in time and not correct report. The other problem that arise that a lot of user participate fore reasonable number that are trying for accessing more hardware resources which are create many difficulties for service provider to achieve that permitting against all request introduced.

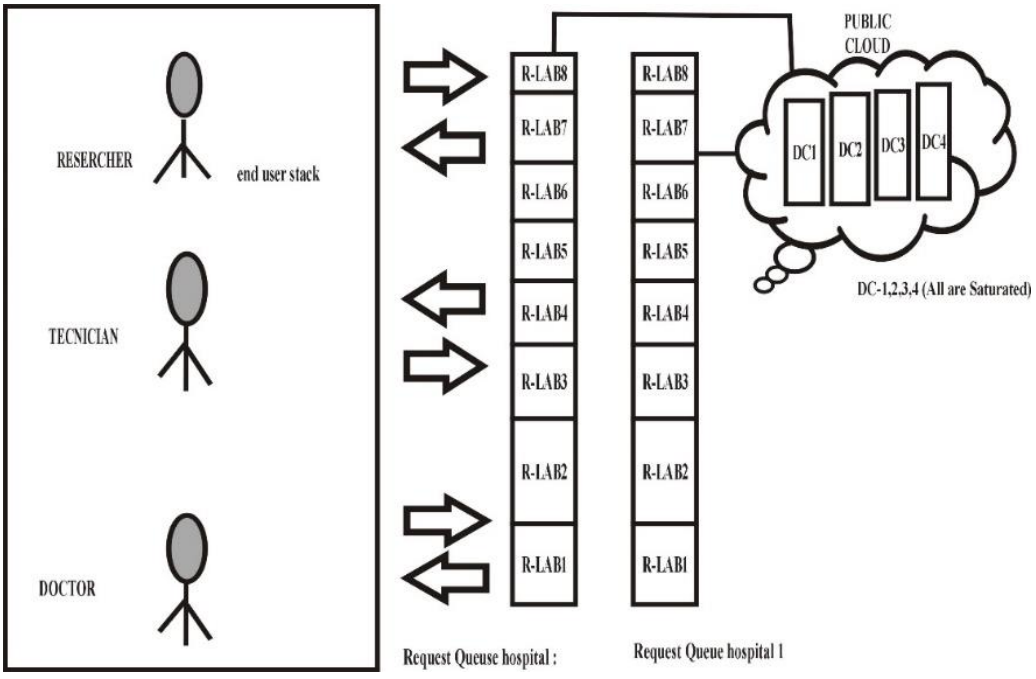

*Figure **3**.11:Public cloud Request-Response Model (RRM)*

The gives situation verified like a visible format figure 3.11 to an enhanced clarification of the genuine issue. To identify the given fig – this study uses open cloud that donate to help from cloud. Possible examination facilities in Medical Image Processing (MEP).

The Public Cloud healthier change in private cloud in superior service purpose, that the private cloud able to provide better responses, security, less time consume networking potential process. Consequently, the framework must be administration for information like a suitable approach, and organization arise needs like rows in a way mode to devote hospitalization in private cloud. Linked in advances related to public cloud for backup also this method in which request line control in a best possible way and information managed batterly on cloud directed as a response to end user that are alleviated. Meanwhile the private cloud provides satisfactory material that modified the devoted hospital conferring for a large number of doctor, employee on expert existing that each doctor has his crossing point in which the whole information about any request and reaction actuality prepared. In future this framework supports mutually for stake holder moreover Service Provider or End user as moderate's period also reply. At the end final user, no more artistic for delaying about information delaying. Therefore, the information handling must be done better way, by assistance the cloud private relatively by subseries on public cloud service tactic.

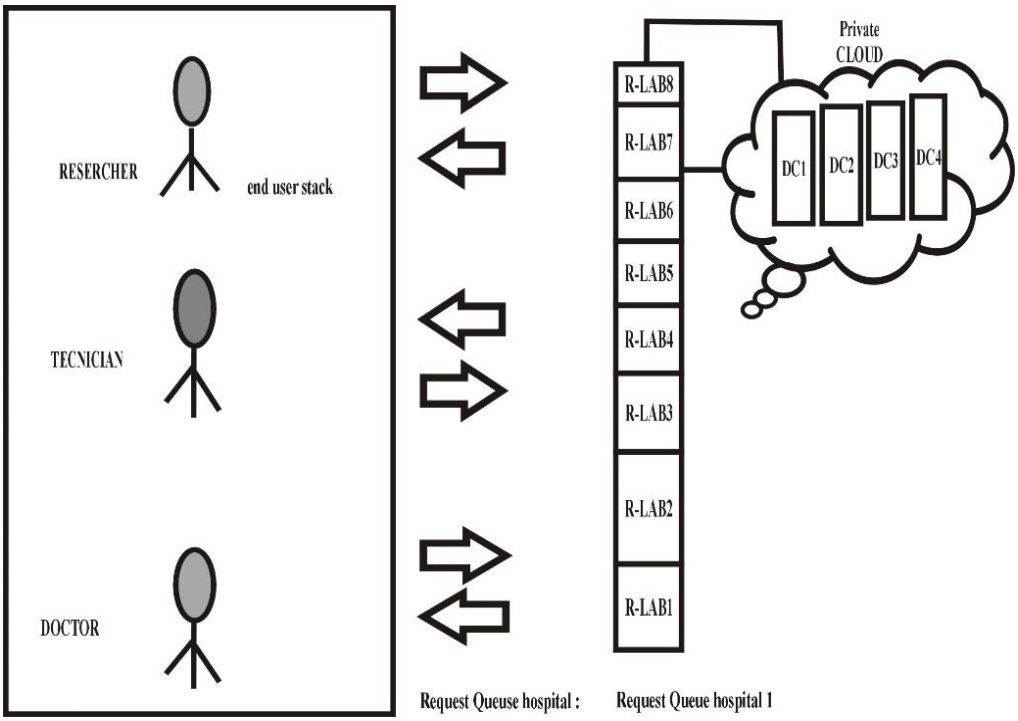

*Figure **3**.12:Cloud Medical Image Processing Framework*

In figure 3.12 we are restrictive the queue to individual the hospital X which has End Users and private cloud. Hospitalization resources has single devoted queue as single request that also create devoted response to hospital X.

3.6.2. Scenario-2

Let's suppose with other example for the Progressive Web Application (PWA) for betterment cloud computing that is applied as the final tool of solution in relatives for accessibility better resources control and collaboration to attain simple solution. Suppose that a concern within provide a complete in local machine that use is no hazards for those who develops to build the alteration in cipher and inter connect with developers thinking point of view of system that is under administered in local machine that has no current simplex synching and collaboration. The client if want to see that fluctuation is allowing to necessity for the change with the time changing that only apparatus to see that whites new thing happen to complete after the changing in system if no invention style. Likewise, for the developers they want to distribute their funds during the period of development with comprises graphically, ciphers and also getting information from every are that work on similar scheme bit harder to deprive of chief apparatus. While each person is compelling cipher important but the reason is that absence of important central server which really cannot accomplish the requirement of the today modern web development that has no extra ordinary function in given scenario. This condition seriously distresses the system the given line time period in term of sources management, that is effect on collaboration between the developers and not cipher synching development is nearby that computer the run batterly for checking it into the server as a client to perform bitterly and faster delivery for better solution to client for use. Again establishes the given scenario in visible content for the healthier appreciative.

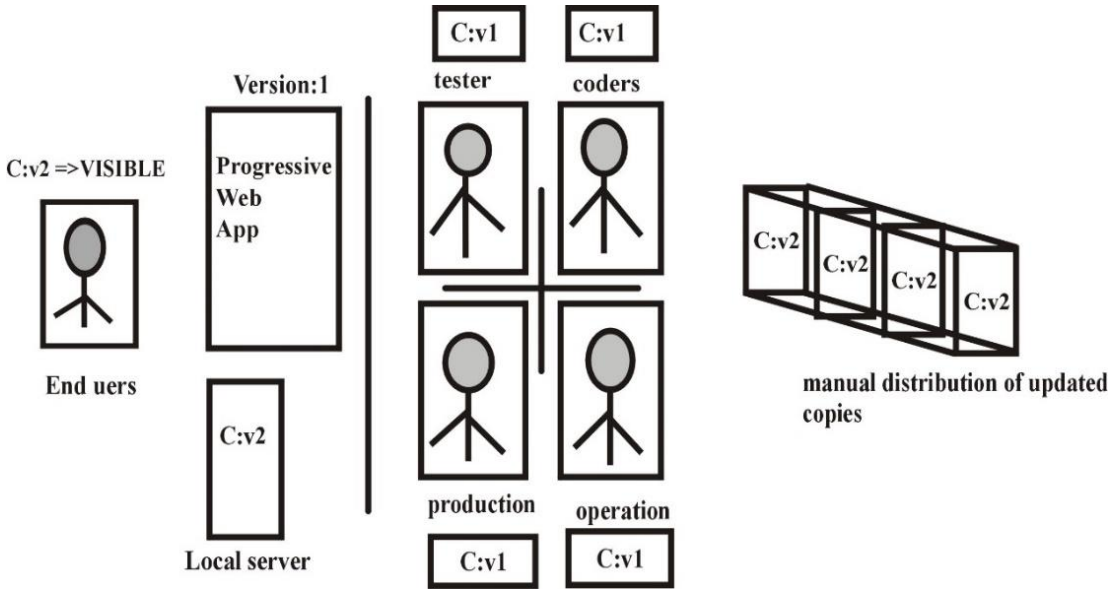

Figure 3.13:Local copies distribution Mechanism

In the figure 3.13 it is evidently marked out that the application up-to- date the copy of form V2 individually simulated that confined server also completion the user in which client is able to sight to update that existence complete the manufacture company includes testing, coders, manufacturing, operation and cipher is physical delivery existing copies complete. That also produce association subjects and reserve organization out of sorts moved by the team of IT.

Now it's time to commence of the solution of all subjects like as cloud mechanism is slightly likely problem solution for that with in the possessions such as cipher version is well begin complete and new inward material are simulated to live UI and also request to clients to see. Collaboration amongst the developers is healthier resolving the problem of teamwork and share of cipher quantity of manufacturing server and different confined body that are leading to cipher.

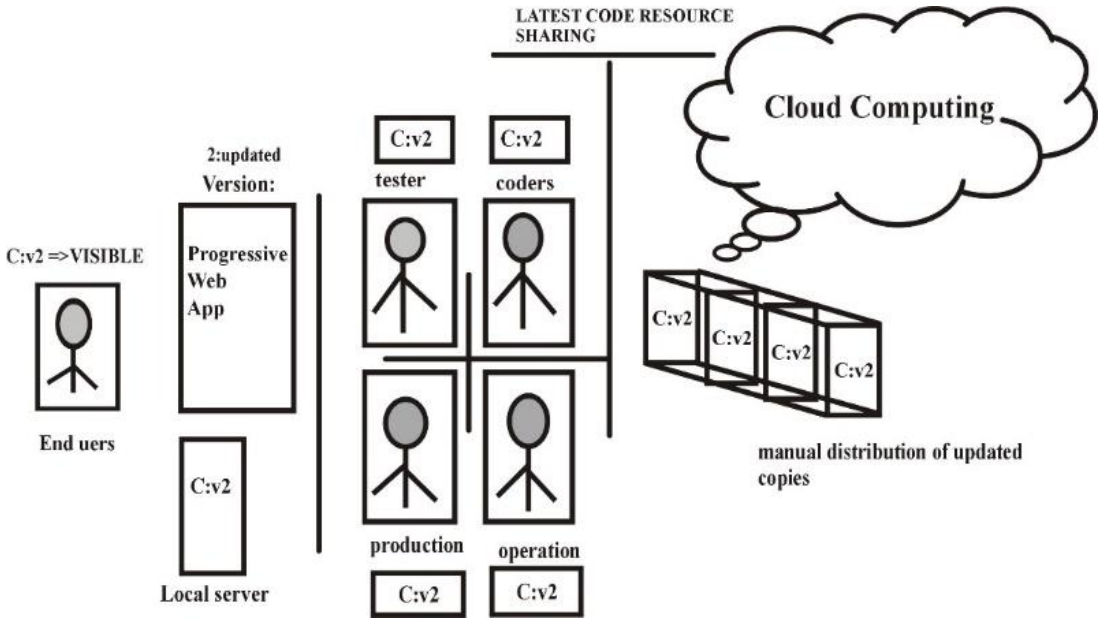

Figure 3.14:Cloud Computing Resource Syncing

The above scenario it is obviously apparent in figure 3.14 cloud is distribution the cipher text source amongst the teams and newest copy of cipher text also very noticeable in whole demesne of the Progressive Web Application (PWA) that also syncing the cipher text that is impulse and stress operation also achieved from the team's point of view. That method of integrating cloud computing surrounding with geographical teams of development delivers to influence wait daily runs to offer. Due to this it saving time, money and time collaboration also increasing efficiency and user's gratification.

3.7. Summary

Security evaluation and assessment is a process for implementation of security control with constantly reviewing identification of security vulnerabilities and threats. In this chapter granular detailed methodology for security framework for evaluation of security controls on cloud. This thesis proposed a framework for secure cloud computing environment that perform the identification of security requirements, attacks, threats and concerns associated to deployment of the clouds. This framework acts in many conditions that check security, privacy, load balancing and trust. In this chapter the AES algorithm is discussed, when the MixColumns stage is switched with a XOR operation to increase the speed of the encryption and decryption algorithm. The time needed for the XOR operation stage will be calculated and compared with the time MixColumns stage. Moreover, the overall time consumption needed for the encryption and decryption process will be measured and compare with the time needed for the AES encryption and decryption processes. The proposed framework is developed using Cloudsim and Ifogsim simulators on Eclipse integrated development environment.

CHAPTER 4

RESULTS AND DISCUSSION

4.1. Overview

The simulation can store and generate a large amount of data. It can allow a user to measure factors like security privacy, energy consumption, network usage, delays, trusted devices and service management. Any new encryption algorithm needs to pass some tests before approving it, these tests ensure that the new scheme will work without problems and don't have any problem in security. These tests are for testing the encryption speed applied on the AES algorithm on framework then the results will be discussed.

4.2. Application Details

The developed application comprises on our proposed framework. We made it generic so that anyone could put one's idea or logic in this application and get the required results. Configurations are so generic; it can help the user to test different scenarios under the proposed algorithm. We have redesigned the simulators according to our application need. The application has the ability to store and generate large amount of data. It can allow a user to measure the factors like security privacy, energy consumption, network usage, delays, trusted devices and service management. The Graphical User Interface of the model is given below.

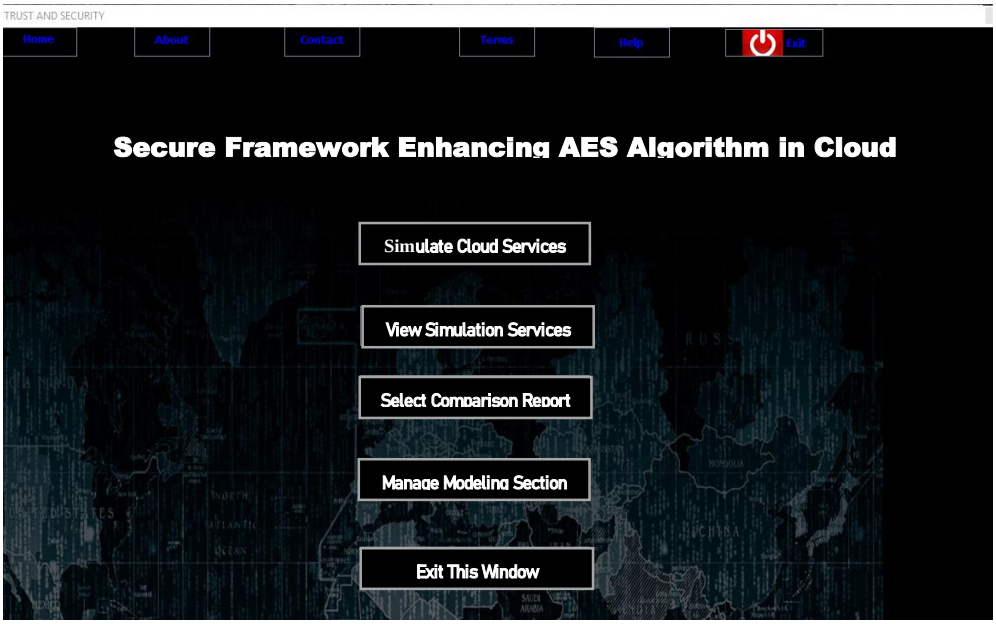

Figure 4.1:Graphical User Interface of the application

4.3. Results and Discussion

In order to check and test the efficiency of the proposed algorithm, a simple code is used. This test helped us to prove that the proposed AES algorithm is better than any other AES algorithm, and after implementation of AES and advanced AES code on hardware will reduce the execution time. The SFCC results as performed and the implementation of this security framework for cloud computing. The period acts as an energetic character during the peers of key, encryption, and decryption procedure. Altogether, inquiries remain complete on Intel(R) Core-i3 with CPU 2.27 GHz processor, 4 GB RAM on Windows 10 at the work framework by using CloudSim with iFogSim as simulators on Eclipse integrated development environment. CloudSim is a very well-known and popular among simulators for cloud-based applications.

Various parameters such as encryption, decryption, energy consumption, network usage, network delay, trusted devices, and service management devices are compared. The same algorithms are implemented in real-time applications to solve the aforementioned issues. The results gathered from the simulations are very accurate. Codes are very consistent with real-time mechanisms. The simulators are redesigned according to the application need. The implementation period is a basic of the spell that is required to change a basic text to an encryption manuscript and vice versa, while encryption time that is referred to the time taken to change a basic text to a ciphertext and decryption which is referred to the time required to convert a cipher text to a plain text are both predicted to be short in instruction to take rapid and approachable system. Moreover, this execution time somehow is contingent on the layout of the system used. Table 4.1 offers the execution period in milliseconds (ms), which is obtained by computing the average encryption/decryption time after encrypting/decrypting the input text in 0.5 MB sizes while using the same key run on 16, 32, 64 and 128 bytes.

Table 4.1:Execution Time Test Result [20]

Plain Text Size	AES	Avrg. Encryption Time(ms)	Avrg. Decryption Time (ms)
16 byte	Existing AES	0.1658	0.1789
	Propose AES	0.1190	0.1481
32 byte	Existing AES	0.2976	0.3114
	Propose AES	0.2507	0.2839
64 byte	Existing AES	0.4564	0.4626
	Propose AES	0.3916	0.4590
128 byte	Existing AES	0.6984	0.5911
	Propose AES	0.6014	0.5805
0.5 mb	Existing AES	2359.65	2269.32
	Propose AES	2159.8	2207.1

Table 4.1 presents the execution time test results in milliseconds (ms), which are attained by computing the average encryption/decryption time after encrypting/decrypting the input text in 0.5 MB sizes of the while using the same key run on 16, 32, 64, and 128 bytes. The results of Figures 4.2, 4.3 and 4.4 specify that the existing AES has a minor rise in the encryption and decryption time after matched to the existing AES algorithm. The percentage different between encryption time of existing and proposed AES for 16 byte, 32 byte, 64 byte and 128 byte are 28.23%, 15.76%,14.20%,16.21% respectively.

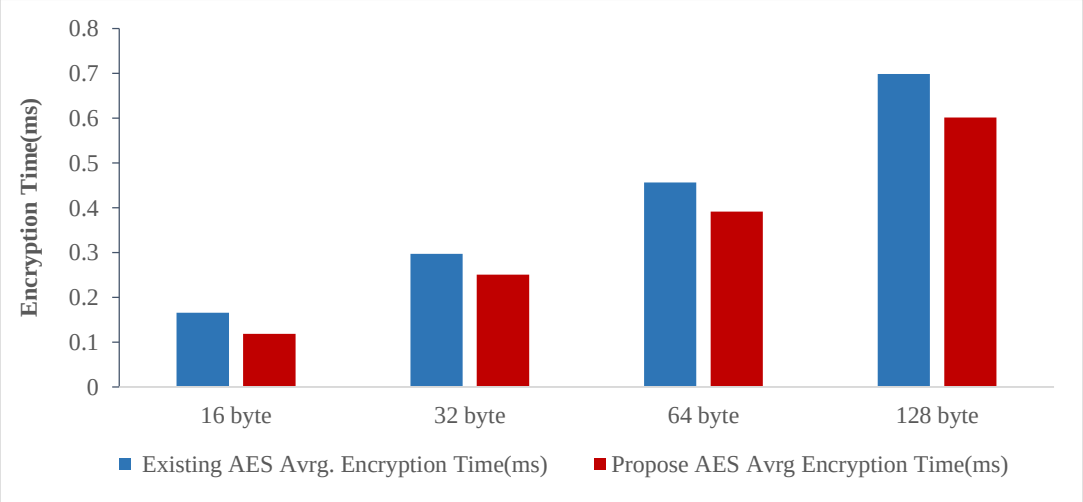

Figure 4.2: Existing AES vs Proposed AES (Encrypting Time)

The percentage different between decryption time of existing and proposed AES for 16 byte, 32 byte, 64 byte and 128 byte are 17.22%, 8.83%,0.78%,9.76% respectively.

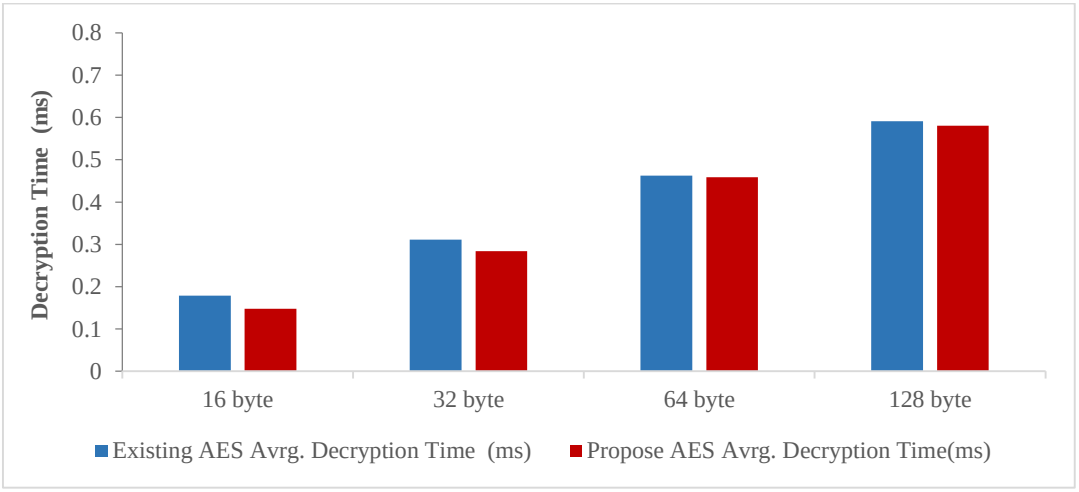

Figure 4.3: Existing AES vs Proposed AES (Decrypting Time)

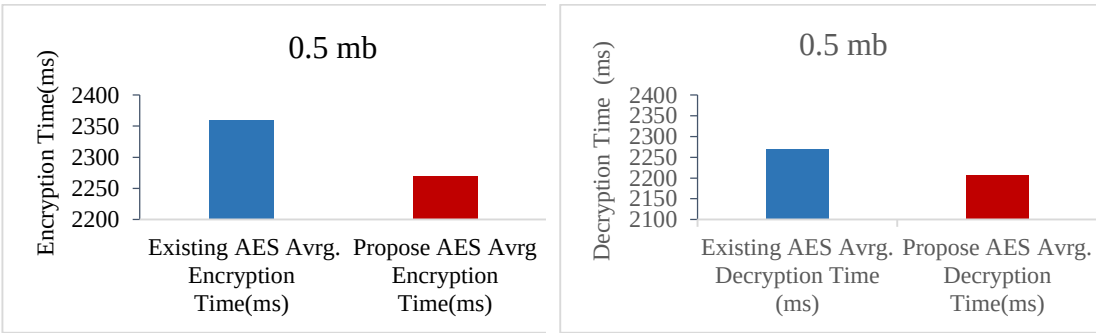

Figure 4.4:Encrypting and Decrypting Time Existing AES vs Proposed AES

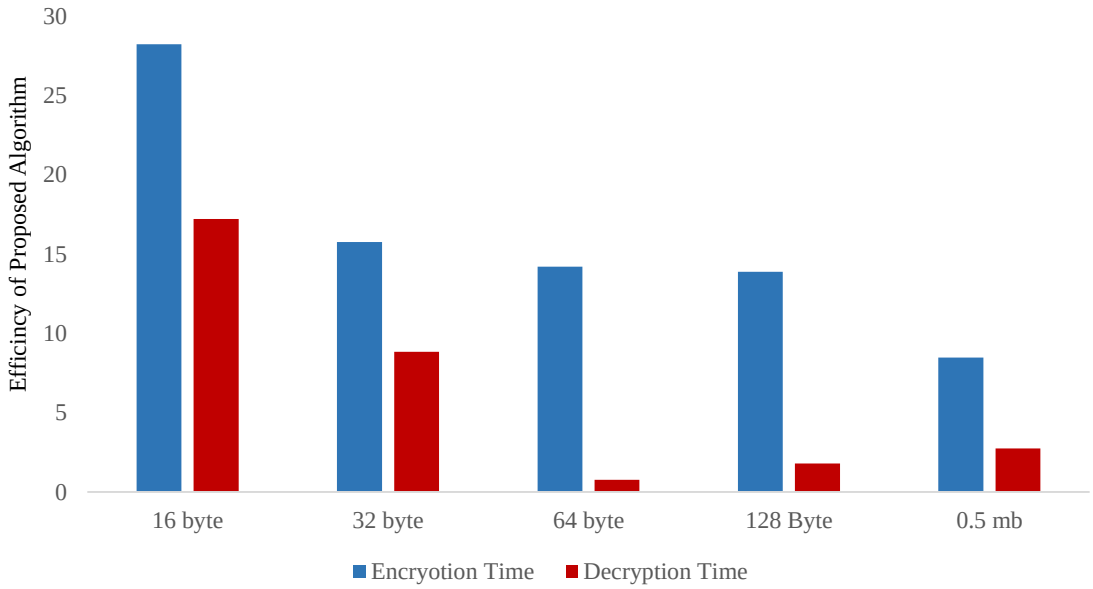

Figure 4.5:Efficincy of Proposed Algorithm Test Result

Comparisons of efficiency of existing and proposed methods showing in Figure 4.5 clearly identify differences of performances in consumption time for each algorithm used to encrypt each transaction type.

4.3.1. Avalanche effect

In cryptography, stuff called dispersal reproduces the cryptographic asset of an algorithm. If there is a small alteration in an input, the output changes meaningfully. This is also called the inundation effect. Avalanche consequence is leisurely by means of pretense reserve. Hamming reserve in material philosophy is the amount of variation. Playacting reserve is the amount of bit-by-bit XOR bearing in mind ASCII value as it develops informal to devise programmatically. A high gradation of dispersal, i.e., extraordinary avalanche consequence, is anticipated. Avalanche's conclusion reproduces the presentation of a cryptographic algorithm. The avalanche effect is described in Table 4.2.

Table 4.2:Avalanche Effect Test Result Obtained After Flipping Single Bit in the Plain Text [20]

Execution Program	Plain Text	Secret Key	Encryption and Decryption Time	Execution Time
First Time Execution	I Love Unimorin!	H2+3S+MuePgIPK3h9SAHOtl6T Htl8ak062IgB3ixEto	Encryption Time	0.05172414
			Decryption Time	0.03448276
Second Execution	I Love Unimorin!	1mRVUf7lRS7W/K+BWFRkP3// KKjf0FtIaSnIGArvudY=	Encryption Time	0.06666667
			Decryption Time	0.044444446

The avalanche effect is described in Figure 4.6 (simulation results from Table 4.2)

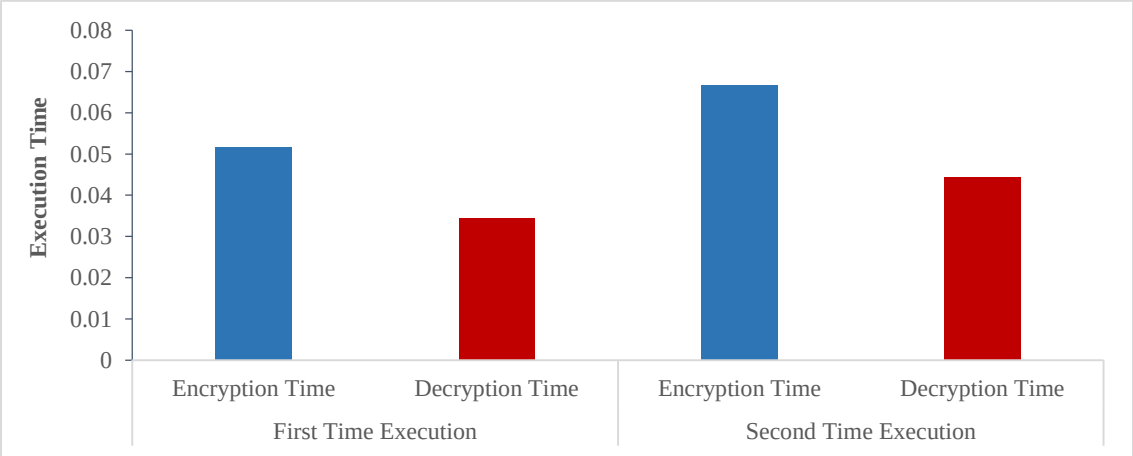

Figure 4.6:Avalanche Effect Test Result

4.3.2. Comparative Analysis of Computed Results with Existing Works

A comparative analysis of computed consequences with the current work is presented as follows. However, some researchers analyzed the performance of their advanced AES version. Meanwhile, many authors used encryption and description time as their performance metrics. The simulation environmental comparison between proposed AES and other AES using the CloudSim simulator is graphically represented in Figures 4.7 and 4.8.

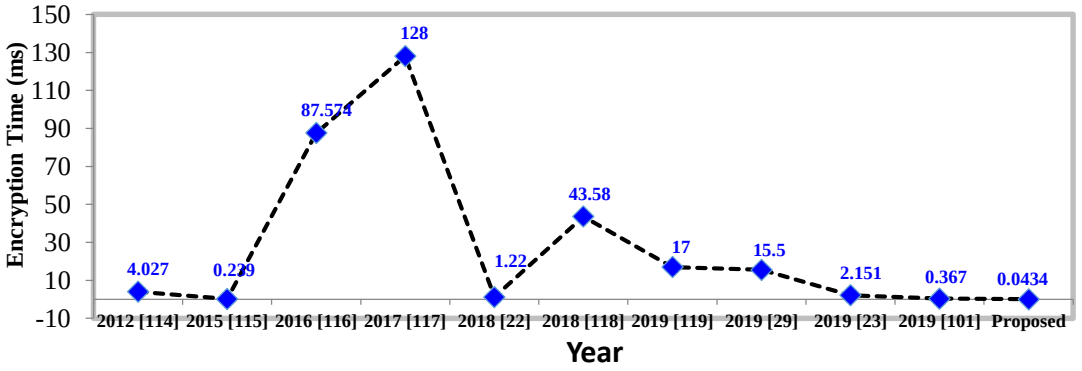

Figure 4.7:Encryption processing time Factor in Different AES

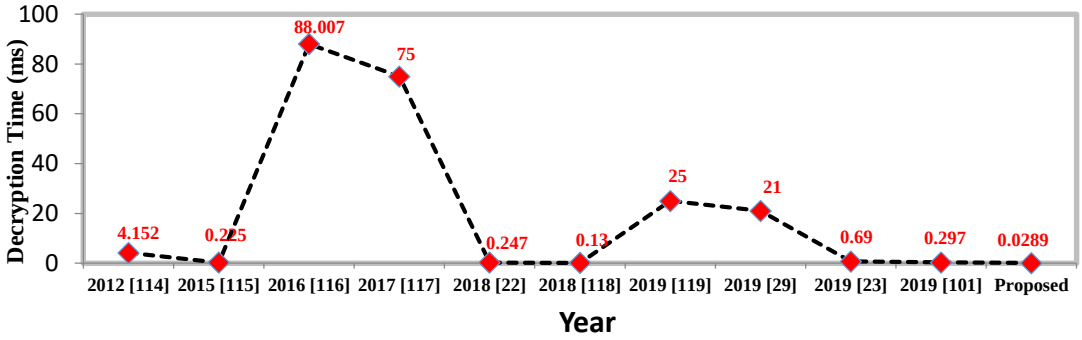

Figure 4.8:Decryption time processing Time Factor in Different AES

4.3.3. Average Energy Consumed

By using the same technique described in [20], the energy consumption is being evaluated. These experiments shared that the proposed frameworks have 14% less energy consumption as compared to [20]. Actual cost taken is given by encryption and the average current that is used by every CPU clock cycle. Equation (4) is used to calculate energy cost per byte as well as various keys of AES encryption schemes:

$$: \sum E = E_c + (T_L - T_c/T_u) - P * M \quad (4)$$

$\sum \mathbf{E}$ represents the Average Energy consumption.

$\mathbf{E_C}$: current energy of host used to accept the data for processing.

$\mathbf{T_L}$ initial time the data was received by the host.

$\mathbf{T_c}$ current time of the data under processing.

$\mathbf{T_u}$ final time of data after finishing the processing and forwarding it to next hop.

where C, L. and u represent the current, last, and updated, respectively.

The energy consumption E is the amount of work done on processing Mips M under a time frame T using power model. The mathematical notation to represent the energy consumption is described in Figure 4.9.

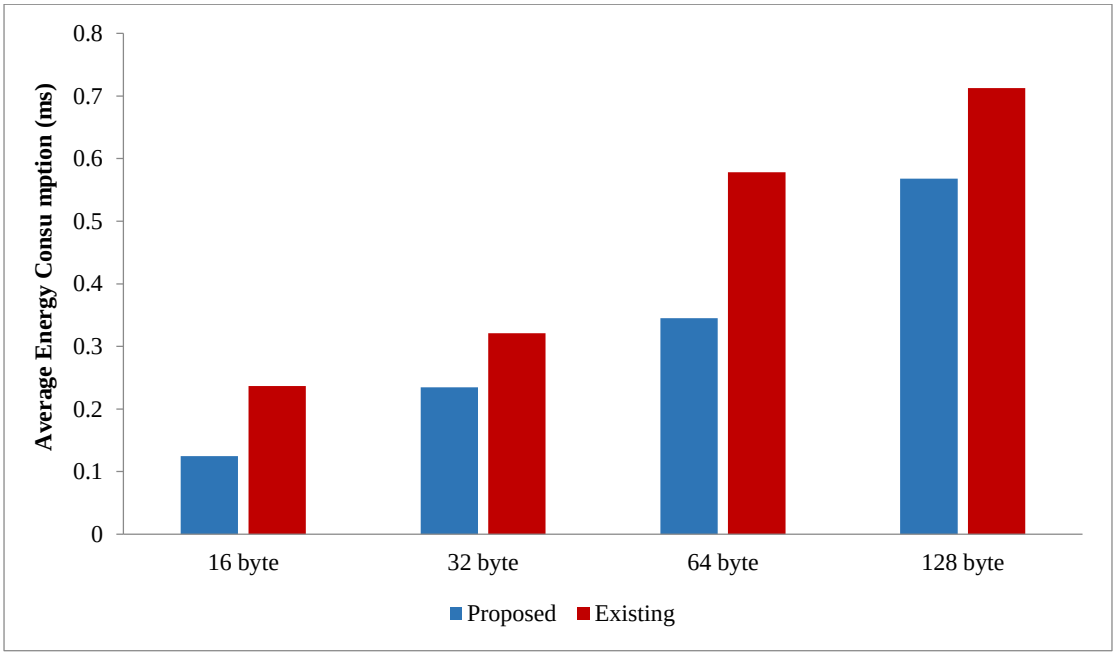

Figure 4.9:Energy consumption for different keys AES Encrypting and Decrypting

4.3.4. Average Network Usage

Network usage is the overall network usage for the system. Network usage is represented in kilobytes. This parameter defines the usage of network resources. The length is reduced and approaches of requests to lower hierarchy by using service configuration so that the request could be processed in the lower hierarchy rather than sending it to cloud again and again. This algorithm reduces 3-hop communication to single-hop communication. Thus, low network usage is obtained through the proposed framework. The more the network is used, the more the expenditure. Efficient network topologies prefer to use minimal network. In these experiments, the network usage is evaluated using the same technique described in [20]. In the proposed framework, network resources are reduced by 11% as compared to [20]. The network while running the implemented encryption schemes is calculated using the following equation:

$$: \sum \mathrm{Nu} = \mathrm{Ni} + (\mathrm{L} * \mathrm{D} * \mathrm{B})/\mathrm{T} \quad (5)$$

here Ni is the initial network usage (Nu at 0).

The network usage mathematical notation Nu is the number of bits B communicated in a certain time frame on devices under sets of data D with latency L. Simulation result is clear from Figure 4.10.

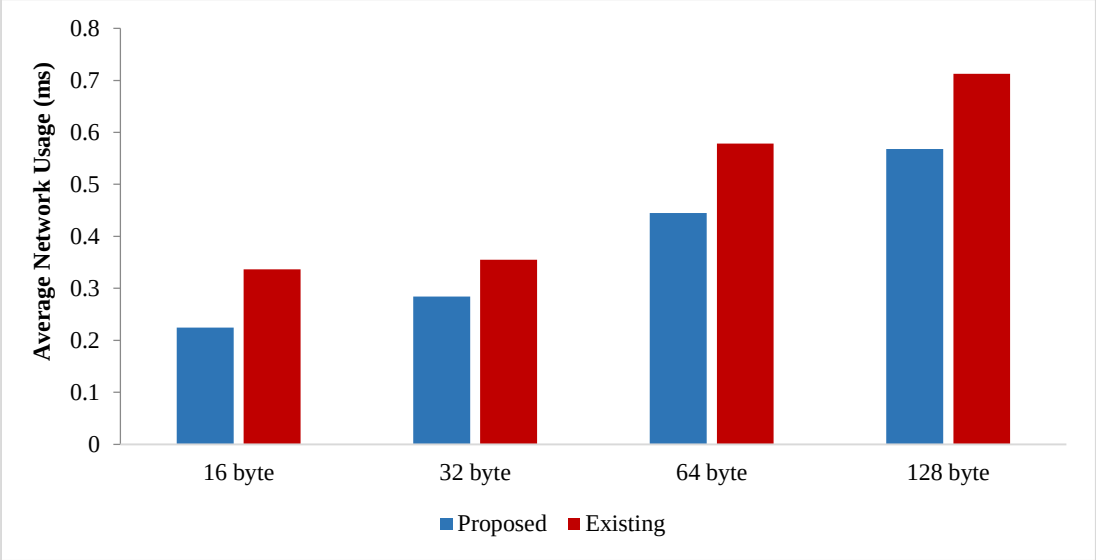

Figure 4.10:Network usage for different keys AES Encrypting and Decrypting

4.3.5. Average Networking Delay

In the calculation of testing and evaluating whether the data are secured, delay is likewise evaluated. In the local host cloud environment amount of consumers; the data traffic will develop tall, which will have influence on the scheme. In a real environment, numerous issues could cause delays, e.g., the size of the key and network speeds, which will cause suspensions and overcrowding. The larger numbers of key indicate increased delay due to the time when more data encrypt generate. When the key, it is originally split into dissimilar blocks formerly encryption. The scope of individual block may have contingent influence on the scope. The delay comparison of the previous methodology [20] and the research shows that the significant differences in the delay indicate that the proposed framework is 15% better than the previous solution [20].

$$\sum D_n = B_s * L/T - B_d * L/1 - T/T_e \quad (6)$$

The delay D represents the time that the bits B take to reach a processing device from an end device under a certain latency L and connection time T. The observed delay is calculated using the equation. The mathematical notation to represent the delay is described below and by simulation result it is clear from figure. The delay calculation is shown in Figure 4.11.

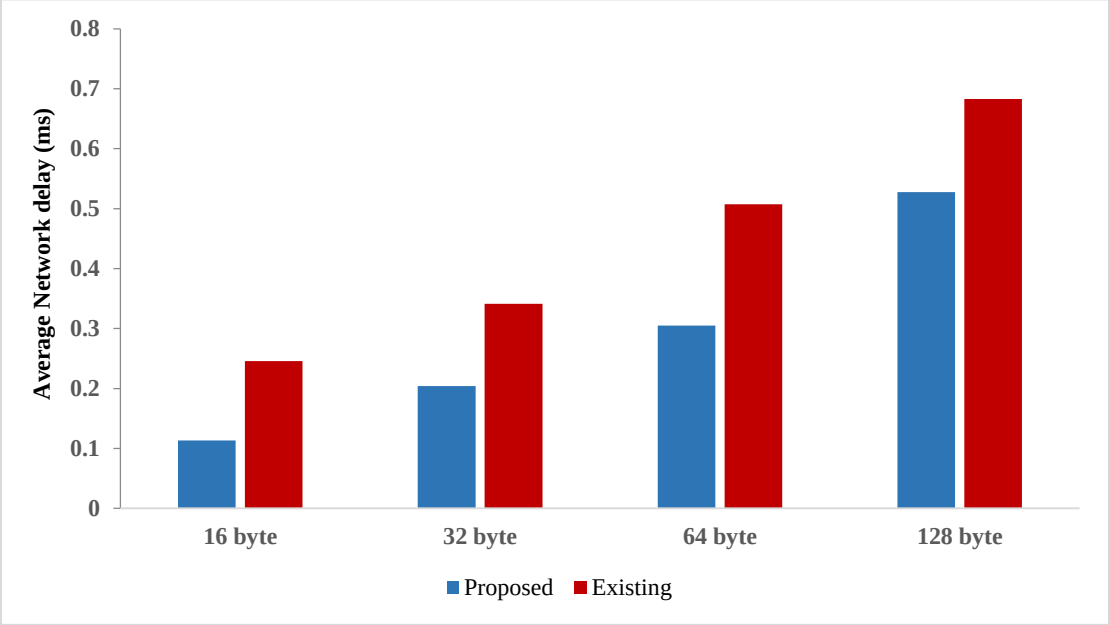

Figure 4.11:Networking Delay for different keys AES Encrypting and Decrypting

4.4. Summary

To provide data confidentiality and information integrity of users' data in the cloud computing environment, an effective security framework is proposed that provides a mechanism through which communication is protected and unauthorized access is restricted. The proposed security framework allows cloud users to securely handle the privacy and integrity of data. It also allows Security, Privacy, network usage and storage in the cloud without depending on the plausibility of the cloud provider. The application of the AES algorithm world provides a strong foundation that protects data stored in the cloud as well as authorizes access to data only on successful authentication and verification. The delays that occur in the actual environment vary to different situations which all are not considered in this framework. Simulation results are visualized in a way that depicts suitability of the algorithm while achieving particular quality attributes. Results show that the proposed framework of AES with 16, 32, 64, and 128 plain text bytes minimizes, energy consumption by 14.43%, network usage by 11.53%, and delay by 15.67%. Hence, the proposed framework enhances security, minimizes resources utilization and reduces delay while deploying services of computational clouds.

CHAPTER 5

CONCLUSIONS AND FUTURE WORK

5.1. Conclusions

To solve the security related problems this research has presented solution i.e Access Control and presented different methods that can be used in real time and to secure the cloud environment. To provide data confidentiality and information integrity of users' data in the cloud computing environment, an effective security framework is proposed that provides a mechanism through which communication is protected and unauthorized access is restricted. The proposed security framework allows cloud users to securely handle the privacy and integrity of data.

There should be a verification process for security solutions before they are deployed in any organization. A real time environment run is necessary before the deployment of these solutions just to make sure whether these are working properly or not. As technology is developing day by day and there has been seen a switch from traditional computing to cloud computing, so the threats which are identified in this research has calculated in that technological shift scenario therefore this solution is presented for deployment of new cloud computing models. The proposed solution has been verified with performance perspective within including network, data packet and resources utilization. We can conclude from the analysis and proposed framework is a reliable solution of the above mentioned issues. These experiments are performed in state of the art simulation environment under the supervision of qualified experts of Cloud Computing field. The research work aims to solve the issues of Security, Privacy, Trust and Load Balancing immediately.

To provide data confidentiality and information integrity of users' data in the cloud computing environment, an effective security framework is proposed that provides a mechanism through which communication is protected and unauthorized access is restricted. Also, a framework with key features including enhanced security and owner's data privacy is presented. It allows Security, Privacy, network usage and storage in the cloud without depending on the plausibility of the cloud provider. The application of the AES algorithm world provides a strong foundation that protects data

stored in the cloud as well as authorizes access to data only on successful authentication and verification. The delays that occur in the actual environment vary to different situations which are not considered in this framework. Simulation results are visualized in a way that depicts suitability of the algorithm while achieving particular quality attributes. Results show that the proposed framework of AES with 16, 32, 64, and 128 plain text bytes minimizes, energy consumption by 14.43%, network usage by 11.53%, and delay by 15.67%. Hence, the proposed framework enhances security, minimizes resources utilization and reduces delay while deploying services of computational clouds.

5.2 Future Work

In future, the framework can propose further improvement in the encryption/decryption module by providing high security and low cost computation. It is highly effective and productive for the world of cloud computing. The major concern is to make faster data transmission and processing. From now on SFCC algorithm can be implemented in hardware that may produce preferable outcome. The main target would be on reducing the consumption of the communication and computation resources. The major computation consumption in the proposed solution occurs from the encryption /decryption operations and the adding/verifying of the integrity and authenticity.

REFERENCES

[1]. M. E. Lantarci and H. T. Mouftah, "Enery-Efftecient information and communication infrastructures in the smart grid: A survey on interactions and open issues", *IEEE communications Surveys & Tutorials*, 17(1):179-197,2015.

[2]. S. Aldossary and W. Allen, "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions", *(IJACSA) International Journal of Advanced Computer Science and Applications,* Vol. 7, No. 4, 2016.

[3]. J. Silki and V. Abhilasha, "An improved security framework for cloud environment using ECC algorithm", *International Journal for Research in Applied Science & Engineering Technology*, vol. 6, no. 1, 2018.

[4]. M. M. Dawoud, G. A. Ebrahim and S. A. Youssef, "A Cloud Computing Security Framework Based on Cloud Security Trusted Authority", INFOS '16, May 09-11, Giza, Egypt © 2016 *ACM*.

[5]. S. Ahmad and Dr. M. M. Afzal, "A Study and Survey of Security and Privacy issues in Cloud Computing", *International Journal of Engineering Research & Technology (IJERT),* ISSN: 2278-0181, IJERTV6IS010311, Vol. 6 Issue 01, January-2017.

[6]. G. S. Mahmood, D. J. Huang and B. Abdul rahman Jaleel, "Achieving an Effective, Confidentiality and Integrity of Data in Cloud Computing", *International Journal of Network Security*, Vol.21, No.2, PP.326-332, Mar. 2019.

[7]. Othman, S. Riaz and A. S., "A User-Based Trust Model for Cloud Computing Environment", *International Journal of Advanced Computer Science and Applications*, Volume. 9, 2018.

[8]. Firman, A. Meyliana, Achmad and N.H. Harjanto, P., "Critical Components of Security Framework for Cloud Computing Community: A Systematic Literature Review", *International Journal of Pure and Applied Mathematics,* Volume 118, 2018.

[9]. K,V.Pradeep, V.Vijayakumar and V.Subramaniyaswamy,"An Efficient Framework for Sharing a File in a Secure Manner Using Asymmetric Key Distribution Management in Cloud Environment", *Hindawi, Journal of Computer Networks and Communications,* Volume 2019.

[10]. Dr. R. Sugumar and K. A. M. Joycee, "FEDSACE: A Framework for Enhanced User Data Security algorithms in Cloud Computing Environment", *International Journal on Future Revolution in Computer Science & Communication Engineering,* Volume: 4 Issue: 3, March 2018.

[11]. M. Kpelou and K. Kishore," Lightweight Security Framework for Data Outsourcing and Storage in Mobile Cloud Computing", *International*

Journal of Recent Technology and Engineering (IJRTE), ISSN: 2277-3878, Volume-8 Issue-2, July 2019.

[12]. S. Balamurugan and Dr. S. Sathyanarayana, "Enhanced Security as a Service to Protect Data in Public Cloud Storage", *International Journal of Advanced Research in Computer and Communication Engineering,* Vol. 5, Issue 4, April 2016.

[13]. B. P. Kavin, S. Ganapathy , U. Kanimozhi and A. Kannan," An Enhanced Security Framework for Secured Data Storage and Communications in Cloud Using ECC, Access Control and LDSA", *Wireless Personal Communications* (2020).

[14]. J. R. Jain and A. Asaduzzaman, "A Novel Data Logging Framework to Enhance Security of Cloud Computing", ©2016 *IEEE.*

[15]. J. Singh, "Framework for Client Side AES Encryption Technique in Cloud Computing", *IJIRMPS,* Volume 6, Issue 5, 2018.

[16]. S. Chandel, G. Yang and S. Chakravarty, "AES–CP–IDABE: A Privacy Protection Framework against a DoS Attack in the Cloud Environment with the Access Control Mechanism", *information* 2020, *www.mdpi.com/journal/information*.

[17]. I. A. Elgendy, W. Zhang and Member IEEE, Chuan-Yi Liu, and Ching-Hsien Hsu, senior, "An Efficient and Secured Framework for Mobile Cloud Computing", *IEEE Transactions on Cloud Computing*, 2018.

[18]. W Tsai, Z Jin, and X. Bai, "Internet ware computing: issues and perspective", In: Proceedings of the first Asia-Pacific symposium on Internet ware., pp. 1–10., 2009.

[19]. R. Saha, G. Geetha, G. Kumar, and T.h. Kim, "RK-AES: an improved version of AES using a new key generation process with random keys", *Security and Communication Networks*, vol. 2018, Article ID 9802475, 11 pages, 2018.

[20]. O. C. Abikoye, A. D. Haruna, A. Abubakar, N. O. Akande, and E. O. Asani, "Modified advanced encryption standard algorithm for information security", *Symmetry,* vol. 11, no. 12, p. 1484, 2019.

[21]. K.-L. Tsai, Y.L. Huang, F.-Y. Leu, I. You, Y.-L. Huang, and C.-H. Tsai, "AES-128 based secure low power communication for LoRaWAN IoT environments", *IEEE Access*, vol. 6, pp. 45325–45334, 2018.

[22]. M.V. C. Suana, A. M. Sison, C. Aragon, and R. P. Medina, "Enhancement of advanced encryption standard (AES) cryptographic strength via generation of cipher key-dependent S-box", *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, vol. 6, no. 4, 2018.

[23]. S. Nur Rachmat, "Performance analysis of 256-bit AES encryption algorithm on android smart phone", *IOP Conf. Series: Journal of Physics: Conf. Series,* vol. 1196, 2019.

[24]. A. Oussama and Z. Abdelha, "A security framework for cloud data storage (CDS) based on agent", *Applied Computational Intelligence and Mathematical Methods, Springer, Berlin, Germany*, 2019.

[25]. H. J. Muhasin, R. Atan, M.A. Jabar, and S. Abdullah, "Cloud computing sensitive data protection using multi layered approach", *in Proceedings of the 2016 2nd International Conference on Science in Information Technology (ICSITech),* pp. 69–73, Balikpapan, Indonesia, October 2016.

[26]. K. Ravi and K. B. Rajesh, "Quality based cloud service broker for optimal cloud service provider selection", *International Journal of Applied Engineering Research,* vol. 12, no. 18, pp. 7962–7975, 2017.

[27]. M. Adelmeyer, M. Walterbusch, B. Peter, and T. Frank, "Trust Transitivity and Trust Propagation in Cloud Computing Ecosystems", *Lawrence Erlbaum Associates*, Mahwah, NJ, USA, 2018.

[28]. F. Meng, R. Lin, Z. Wang, H. Zou1, and S. Zhou, "A multi-connection encryption algorithm applied in secure channel service system", *EAI Endorsed Transactions on Security and Safety,* vol. 5, no. 15, 2018.

[29]. H. A. Al Essa and A. S. Ashoor, "Enhancing performance of AES algorithm using concurrency and multithreading", *ARPN Journal of Engineering and Applied Sciences,* vol. 14, no. 11, 2019.

[30]. Andrea Li, "Privacy, Security and Trust Issues in Cloud Computing", *SSRG International Journal of Computer Science and Engineering (SSRG-IJCSE)* – Volume 6 Issue 10 – Oct 2019.

[31]. Dr. K. Sasikala and Mr. M.Annamalai, "Challenges In Cloud Computing on Security Issues And Solutions", *IOSR Journal of Computer Engineering (IOSR-JCE,* (Sep - Oct 2018).

[32]. I.Odun-Ayo, Ananya, M. Frank Agono and Rowland Goddy-Worlu, "Cloud Computing Architecture: A Critical Analysis", ©2018 *IEEE.*

[33]. S. Basu, A.Bardhan, K. Gupta, P.Saha and Mahasweta, "Pal, Manjima Bose, Kaushik Basu,Saunak Chaudhury, Pritika Sarkar", Cloud Computing Security Challenges & Solutions-A Survey" *©2018 IEEE*.

[34]. S. Karimunnisa1, Dr.Vijaya and .S. Kompalli, "Cloud Computing: Review on Recent Research Progress and Issues" , *International Journal of Advanced Trends in Computer Science and Engineering*, Volume 8, No.2, March - April 2019.

[35]. Dr. R. Purohit, "Comparative Analysis of Few Cloud Service Providers Considering Their Distinctive Properties", *International Journal of*

Advanced Research in Computer Science, Volume 8, No. 5, May – June 2017.

[36]. M.N.V Kiranbabu and K.V.V Satyanarayana, "A Perusal Inspection on Ranking the Cloud Service Provider in Cloud Computing", *International Journal of Recent Technology and Engineering (IJRTE)*, Volume-7 Issue-6S2, April 2019.

[37]. P.Verma, A.Gupta and R. S. Sambyal, "Security Issues and Challenges in Cloud Computing: A Review", *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* © 2018 IJSRCSEIT,Volume 4

[38]. M. B. Benjula Anbu Malar and Dr.J. Prabhu, " An Analysis of Security Issues in Cloud Computing", *International Journal of Civil Engineering and Technology (IJCIET)*, Volume 10, Issue 2, February 2019.

[39]. Vaikunth Pai T. and Dr. P. S Aithal, "Cloud Computing Security Issues Challenges and Opportunities", *International Journal of Management, Technology and Social Science*, vol.1, 2017.

[40]. A. Arbaaz Ahmed and Dr. M. I. Thariq Hussan, "Cloud Computing: Study of Security Issues and Research Challenges", *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, Volume 7, Issue 4,April 2018.

[41]. Jahangee Q. and M. I. Maqboo, "Solutions of Cloud Computing Security Issues", *International Journal of Computer Science Trends and Technology (I JCS T)*, vol. 4, no. 2, Mar – Apr 2016.

[42]. Rajeswari, Vinitha and Greeshma, "Survey on Cloud Computing and Security Issues", *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 6, no. 4, April 2018.

[43]. P. Ravi Kumar, P. Herbert Raj and P. Jelciana, "Exploring Security Issues and Solutions in Cloud Computing Services – A Survey", *cybernetics and information technologies*, vol. 17, no 4, 2017.

[44]. X. Dong, J. Yu, Y. Zhu, Y. Chen, Y. Luo, and M. Li, "SECO: Secure and Scalable Data Collaboration Services in Cloud Computing", *Computers & Security*, vol. 50, pp. 91–105, 2015.

[45]. N.Subramanian Research Scholar and A. Jeyaraj, "Recent security challenges in cloud computing", *Computers and Electrical Engineering, Science Direct © 2018 Elsevier.*

[46]. U.Vyshnavi and P.Praveen Yadav, "Trust Management of Cloud Services Using Credibility Assessment Technique", *International Journal of Innovative Research in Science, Engineering and Technology* (An ISO 3297: 2007 Certified Organization) Vol. 5, Issue 10, October 2016.

[47]. K. Gokulnath and R. Uthariaraj, "A Survey on Trust Models in Cloud Computing" , *Indian Journal of Science and Technology,* Vol 9(47), DOI: 10.17485/ijst/2016/v9i47/108685, December 2016.

[48]. M.Payer and T.R. Gross, "Fine-Grained User-Space Security through Virtualization", *Newport Beach, California, USA. Copyright 2011 ACM.*

[49]. C. Platzer, "dAnubis – Dynamic Device Driver Analysis Based on Virtual Machine Introspection", *Conference Paper,* July 2010.

[50]. SaketMaskara, MuditSaraf and Priya, "Trust Management in Cloud Computing", *International Research Journal of Engineering and Technology (IRJET)* e-ISSN: 2395 -0056, Volume: 03 Issue: 11 | Nov -2016.

[51]. R. N. Mrudula and Prof. V. Purushothama Raju, "An Efficient Feedback Based Trust Management Framework for Cloud Computing", *International Journal of Computer Science & Communication Networks,*Vol 7(5),147-151.

[52]. S. Tabassam, "Security and Privacy Issues in Cloud Computing Environment" , *Journal of Information Technology & Software Engineering,* Tabassam, J Inform Tech SoftwEng 2017.

[53]. Nick L. Petroni, Jr., T. Fraser, J. Molina & William A. Arbaugh, "Copilot - a Coprocessor-based Kernel Runtime Integrity Monitor", 2004 by *The USENIX Association.*

[54]. Xiaohui Li, Jingsha He, Bin Zhao, Jing Fang, Y. Zhang, and Hongxing Liang, "A Method for Trust Quantification in Cloud Computing Environments", *Hindawi Publishing Corporation International Journal of Distributed Sensor Networks*, Volume 2016, Article ID 5052614, 7 pageshttp://dx.doi.org/10.1155/2016/5052614.

[55]. Richard D. SHANG, Jianhui Huang, Yinping Yang and Robert J. Kauffman, "Analyzing the Impact of Cloud Services Brokers on Cloud Computing Markets", *Singapore Management University Institutional Knowledge at Singapore Management University*, 2013.

[56]. W. Fan and H. Perros, "A novel trust management framework for multi-cloud environments based on trust service providers", 2014 *Elsevier B.V. All rights reserved.*

[57]. YefengRuan and A. Durresi, "A Trust Management Framework for Cloud Computing Platforms", 2017 IEEE 31st *International Conference on Advanced Information Networking and Applications.*

[58]. M. Oqail Ahmad and RafiqulZaman Khan, "Cloud Computing Modeling and Simulation using CloudSim Environment", *International Journal of Recent Technology and Engineering (IJRTE)* ISSN: 2277-3878, Volume-8 Issue-2, July 2019.

[59]. V.Surya, S.Ranichandra and R.Ranjani, "Secure Cloud Storage Using AES Encryption", *International Journal of Innovative Research in Computer and Communication Engineering* Vol. 6, Issue 6, June 2018.

[60]. Abhijith Nair, SantoshAnand and SomnathSinha, "A Performance Booster for Load Balancing in Cloud Computing with My Load Balancer Technique", *International Journal of Recent Technology and Engineering (IJRTE),* ISSN: 2277-3878, Volume-8, Issue-1, May 2019.

[61]. G.Ali and L.Erwin, "Big Data Security and Privacy Issues in Cloud", *International Journal of Network Security Its Applications*,8(3),59-79,2016.

[62]. N.Ghosh, Student Member, IEEE, Soumya K. Ghosh, Member, IEEE, and Sajal K. Das, Senior Member, IEEE, "SelCSP: A Framework to Facilitate Selection of Cloud Service Providers", *IEEE Transactions On Cloud Computing*, Vol. 3, No. 1, January-March 2015.

[63]. Edjie M. De Los Reyes, Dr. Ariel M. Sison and Dr.Ruji P. Medina., "Modified AES Cipher Round and Key Schedule", *Indonesian Journal of Electrical Engineering and Informatics (IJEEI),* Vol. 7, No. 1, March 2019.

[64]. H. Talirongan, Ariel M. Sison and Ruji P. Medina, "A New Advanced Encryption Standard-Butterfly Effect in Protecting Image of Copyright Piracy", *this publication at: https://www.researchgate.net/publication/* 331663315 , on 06 December 2019.

[65]. A.Arab, M. Javad Rostami and B. Ghavami, "An image encryption method based on chaos system and AES algorithm", *The Journal of Supercomputing,* (2019) 75:6663–6682.

[66]. DiaaSalama and AbdElminaam, "Improving the Security of Cloud Computing by Building New Hybrid Cryptography Algorithms", *IJEIE,* (2018), Vol.8, No.1, pp. 40 - 48.

[67]. D. H. Bui, D. Puschini, S. Bacles-Min, E. Beigné, and X.-T. Tran, "Ultra low-power and low-energy 32-bit datapath AES architecture for IoT applications", *in Proc. Int. Conf. IC Des. Technol. (ICICDT),* pp. 1_4, Jun. 2016.

[68]. Jia H, Liu X, Di X, Qi H, Cong L, Li J and Yang H, "Security Strategy for Virtual Machine Allocation in Cloud Computing", *Procedia computer science*,147:140-4, Jan 1 2019

[69]. M. f. ahmad, M. ali, M.mumtaz Shah and , Munam Ali, "Cryptography: A comparative Analysis for Modern" , *International Journal of Advanced Computer Science and Applications*,8 (6), 442-448,2017.

[70]. M. Marwan, A. Kartit and H. Ouahmane, "A Framework to Secure Medical Image Storage in Cloud Computing Environment", *Journal of Electronic Commerce in Organizations*, vol. 16, no. 1, pp. 1–16, 2018.

[71]. Sirohi, P. and Agarwal, "A: Cloud computing data storage security framework relating to data integrity, privacy and trust", pp. 4–5 (2015).

[72]. Subramanian, K. John and F.L, "Dynamic and secure unstructured data sharing in multi-cloud storage using the hybrid crypto-system", *Int. J. Adv. Appl*. Sci. 2018, 5, 15–23.

[73]. Hany, F. A, Robert J. W. and Gary B.W, "Fog Computing and the Internet of Things: A Review. Big Data Cognitive Computer", 2018.

[74]. M. Alghali, M. A. Najwa and I. Roesnita, "A Framework to Assess Privacy in Cloud Based System", *ARPN Journal of Engineering and Applied Sciences*, FEBRUARY 2016.

[75]. V. Pant, J. Prakash and A. Asthana, "Three Step Data Security Model for Cloud Computing Based on RSA and Steganography Techniques", *In International Conference On Green Computing and Internet of Things (ICGCIoT)* (490-494) IEEE,2015.

[76]. D. Das, A. Bhandari and A. Gupta, "A Framework for Data Security and Storage in Cloud Computing", *In International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), IEEE*,2016.

[77]. V. Dhaka and A. Dhamija, "A Novel Cryptographic and Steganographic Approach for Secure Cloud Data Migration", *In International Conference On Green Computing and Internet of Things (ICGCIoT)* (pp.1-6) IEEE,2015.

[78]. N. Surv, B. Wanve, R. Kamble, S. Patil and J. Katti, "Framework for Client Side AES Encryption Techniques in Cloud Computing", *In International Advance Computing Conference (IACC)*, (525-528), IEEE,2015.

[79]. T. Jiang, X. Chen and J. Ma, "Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation", *IEEE Transactions on Computers*, vol. 65, no. 8, pp. 2363–2373, 2016.

[80]. J. Zhang and X. Zhao, "Efficient Chameleon Hashing-Based Privacy-Preserving Auditing in Cloud Storage", *Cluster Computing*, vol. 19, no. 1, pp. 47–56, 2016.

[81]. G. Yang, J. Yu, W. Shen, Q. Su, Z. Fu, and R. Hao, "Enabling Public Auditing for Shared Data in Cloud Storage Supporting Identity Privacy and Traceability", *Journal of Systems and Software*, vol. 113, pp. 130– 139, 2016.

[82]. A. P. Singh and S. K. Pasupuleti, "Optimized Public Auditing and Data Dynamics for Data Storage Security in Cloud Computing", *Procedia Computer Science*, vol. 93, pp. 751–759, 2016.

[83]. J. Hur, D. Koo, Y. Shin and K. Kang, "Secure Data Deduplication with Dynamic Ownership Management in Cloud Storage", *IEEE Transactions on Knowledge and Data Engineering*, vol. 28, no. 11, pp. 3113–3125, 2016.

[84]. J. Stanek and L. Kencl, “Enhanced Secure Thresholded Data Deduplication Scheme for Cloud Storage”, *IEEE Transactions on Dependable and Secure Computing*, 2016.

[85]. J. Wang, X. Chen, J. Li, J. Zhao, and J. Shen, “Towards Achieving Flexible and Verifiable Search for Outsourced Database in Cloud Computing”, *Future Generation Computer Systems*, 2016.

[86]. R Senthilnathan and Dr.M.Nithya, “A Trust Model and Quality of Service Based Heuristic Scheduling in Cloud Using Genetic Algorithm”, *International Journal of Pure and Applied Mathematics*, Volume 119, No. 16, 2018.

[87]. VangaOdelu, A.K Das, M. Khurram Khan, Kim-Kwang R Choo and Minho Jo, “Expressive CP-ABE Scheme for Mobile Devices in IoT Satisfying Constant-Size Keys and Ciphertexts", *IEEE Access* Vol. 5 2017.

[88]. I. Nakagawa and S.ShimojoZhitao Guan, “IoT Agent Platform mechanism with Transparent Cloud Computing Framework for improving IoT Security" , *IEEE 41st Annual Computer Software and Applications Conference*, 2017.

[89]. B.Mukherjee, R. Lal Neupane and P. Calyam, “End-to-End IoT Security Middleware for Cloud-Fog Communication" , *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing*.

[90]. Q. Huang, Y. Yang and Licheng Wang, “Secure Data Access Control with Ciphertext Update and Comptation Outsourcing in Fog Computing for Internet of Things”, *IEEE Access Journal*, vol. 5, 2017.

[91]. Kai Fan, Qi Luo, Hui Li and Yintang Yang, “Cloud-based Lightweight RFID Mutual Authentication Protocol", *IEEE Second International Conference on Data Science in Cyberspace*, 2017.

[92]. P.K.Dhillon and S. Kalra, “A lightweight biometrics based remote user authentication scheme for IoT services", *Elsevier Journal of Information Security and Applications* 2017.

[93]. S.Raza, T.Helgason, PanosPapadimitratos and T.Voigt, “SecureSense: Ed-to-end secure communication architecture for the cloud-connected internet of things" , *Future Generation Computer Systems, Elsevier* 2017.

[94]. Lin, S., Zhang, R., Ma, H., and Wang, M., “Revisiting attribute-based encryption with verifiable outsourced decryption”, *IEEE Transactions on Information Forensics and Security*, 10(10), 2119–2130, (2015).

[95]. Wang, S., Zhang, Y., and Zhang, Y, “A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems”, *IEEE Access*, 6, 38437–38450, (2018).

[96]. Chatterjee, A., and Sengupta, I., “Translating algorithms to handle fully homomorphic encrypted data on the cloud”, *IEEE Transactions on Cloud Computing*, (2018). 6(1), 287–300.

[97]. Ferretti, L., Marchetti, M., Andreolini, M. and Colajanni, M., "A symmetric cryptographic scheme for data integrity verification in cloud databases", *Information Sciences*, (2018). 422, 497–515.

[98]. Chowdhury, A.R. Mahmud, J. Raihan, A. Kamal and M. Hamid A, "MAES: Modified Advanced Encryption Standard for Resource Constraint Environments". *In Proceedings of the IEEE Sensors Applications Symposium (SAS), Seoul, Korea*, 12–14, pp. 2–7, March 2018.

[99]. Subhash CP, Sumit J, Ravi S and Jyoti C, "Access control framework using multi-factor authentication in cloud computing", *International*, 9(2):1-15, July 2018.

[100]. Bin, S., and Haopu, Y. "Research of fine grit access control based on time in cloud computing", *In 3rd information technology, networking, electronic and automation control conference (ITNEC 2019)* (pp. 1897–1902).

[101]. O. I. Omotosho, "A review on cloud computing security", *International Journal of Computer Science and Mobile Computing, IJCSMC*, vol. 8, no. 9, pp. 245–257, 2019.

[102]. Kumari A, Kumar V and Abbasi MY, et al. "Csef: cloud-based secure and efficient framework for smart medical system Using ECC", *IEEE Access*, 8:107838–107852, 2020;

[103]. Akber A.K, Vinod K,Musheer .A, Saurabh .R and Dheerendra .M, "PALK: Password-based anonymous lightweight key agreement framework for smart grid", *Electrical Power and Energy Systems, Elsevier* 2020.

[104]. Mishra D, Kumar V and Dharminder D, et al. "Sfvcc: Chaotic map-based security framework for vehicular cloud computing", *IET Intelligent Transport Syst*. 2020;14(4):241–249.

[105]. Felicisimo V and Wenceslao, Jr. "Enhancing the Performance of the Advanced Encryption Standard(AES)Algorithm Using Multiple Substitution Boxes", *International Journal of Communication Networks and Information Security (IJCNIS),* Vol. 10, No. 3, December 2018.

[106]. Ugba T. Pius, Eze C. Onyebuchi, Ogidi P. Chinasa and Ekle F. Adoba, "A Cloud-Based Data Security System using Advanced Encryption (AES) and Blowfish algorithms", *Journal of Scientific and Engineering Research,* 2018.

[107]. Calheiros, R. N., Ranjan, R., Beloglazov, A., De Rose, C. A., and Buyya, R. "CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms", *Software: Practice and experience*, (2011). 41(1), 23-50.

[108]. Gupta, Harshit, et al. "iFogsim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things, Edge and Fog computing environments", *Software: Practice and Experience* 47.9 (2017): 1275-1296.

[109]. B. T. Spiers, M. Halas, R. A. Schimmel, and D. P. Provencher, "Secure network cloud architecture", *U.S. Patent 8,984,610, United States Patent (Justia Patents),* 2015.

[110]. E. Bertino, F. Paci, R. Ferrini, and N. Shang, "Privacy-preserving digital identity management for cloud computing", *IEEE Data Engineering Bulletin*, vol. 32, no. 1, pp. 21–27, 2009.

[111]. S. Yi, Li Cheng, and Q. Li, "A survey of fog computing: concepts, applications and issues", *in Proceedings of the 2015 Workshop on Mobile Big Data, pp. 37–42, ACM, Hangzhou, China*, June 2015.

[112]. M. Aazam and E.-N. Huh, "Fog computing and smart gateway based communication for cloud of things", *in Proceedings of the 2014 International Conference on Future Internet of Bings and Cloud*, pp. 464–470, IEEE, Barcelona, Spain, August 2014.

[113]. G. N. Selimis, A. P. Kakarountas, A. P. Fournaris, A. Milidonis, and O. Koufopavlou, "A low power design for sbox cryptographic primitive of advanced encryption standard for mobile end-users", *Journal of Low Power Electronics*, vol. 3, no. 3, pp. 327–336, 2007.

[114]. R. Paul, S. Saha, S. Sau, and A. Chakrabarti, "Design and implementation of realtime AES-128 on real time operating system for multiple fpga communication", 2012, http://arxiv. org/abs/1205.2153.

[115]. L. R1 and H. S2 Mohan, "Implementation and performance analysis of modified AES algorithm with key-dependent dynamic S-box and key multiplication", *Computer Applications Research,* vol. 5, no. 3, 2015.

[116]. D. Lohit Kumar, Dr.A. R. Reddy, and S. A. K. Jilani, "Implementation of 128-bit AES algorithm in MATLAB", *International Journal of Engineering Trends and Technology (IJETT),* vol. 33, no. 3, 2016.

[117]. M. A. FaiqaMaqsood, M. M. Ali, and M. Ali Shah, "Cryptography: a comparative analysis for modern techniques", *International Journal of Advanced Computer Science and Applications,* vol. 8, no. 6, 2017.

[118]. F. Meng, R. Lin, Z. Wang, H. Zou1, and S. Zhou, "A multi connection encryption algorithm applied in secure channel service system", *EAI Endorsed Transactions on Security and Safety*, vol. 5, no. 15, 2018.

[119]. Dr. N. Suba Rani, Dr. A. Noble Mary Juliet, and K. Renuka Devi, "An image encryption & decryption and comparison with text - AES algorithm", *International Journal of Scientific & Technology Research*, vol. 8, no. 7, 2019.