Trusted Cloud Service Framework to Secure Cloud Computing

A thesis

Submitted for the award of the degree of
Doctor of Philosophy
in

Computer Science & Engineering

By

Chandrajeet Yadav
Enrollment No. - MUIT0117038038

Under the Super vision of

Dr. B.D.K Patro
Associate Professor
Rajkiya Engineering College, Kannauj

Under the Co-Supervision of

Dr. Vikash Yadav
Assistant Professor
A.B.E.S Engineering College, Ghaziabad.

Computer Science and Engineering Department
Maharishi University of Information Technology
Sitapur Road, P.O. Maharishi Vidya Mandir
Lucknow, 226013

September 2021

CERTIFICATE

This is to Certify that the entitled **"Trusted Cloud Services Framework to Secure Cloud Computing"** Submitted to Department of Computer Science & Engineering, Maharishi University of Information Technology, Lucknow, Uttar Pradesh , in fulfilment of the requirement for award of degree of 'Doctor of Philosophy' in Computer Science & Engineering, embodies the original work carried out by **Mr. Chandrajeet Yadav**, Under my supervision and not been submitted in part of full for any degree or diploma of this or any other University. It is further certified that scholar fulfils all the requirements as per ordinance of the University for the purpose of submission of Ph.D. thesis.

(Dr. B.D.K Patro)
Supervisor

CERTIFICATE

This is to Certify that the entitled **"Trusted Cloud Services Framework to Secure Cloud Computing"** Submitted to Department of Computer Science & Engineering, Maharishi University of Information Technology, Lucknow, Uttar Pradesh , in fulfilment of the requirement for award of degree of 'Doctor of Philosophy' in Computer Science & Engineering, embodies the original work carried out by **Mr. Chandrajeet Yadav**, Under my supervision and not been submitted in part of full for any degree or diploma of this or any other University. It is further certified that scholar fulfils all the requirements as per ordinance of the University for the purpose of submission of Ph.D. thesis.

(Dr. Vikash Yadav)
Co-Supervisor

DECLARATION

I, hereby declare that the work presented in this thesis entitled **"Trusted Cloud Services Framework to Secure Cloud Computing"** in fulfilment of the requirement for award of degree of 'Doctor of Philosophy' in Computer Science & Engineering, of Maharishi University of Information Technology, Lucknow, Uttar Pradesh, is an authentic record of my own research work carried out under the supervision of **Dr. B.D.K Patro**, Associate Professor, Rajkiya Engineering College, Kannauj and **Dr. Vikash Yadav**, Assistant Professor, ABES Engineering College, Ghaziabad.

I also declare that the work embodied in the present thesis is my original work and has not been submitted by me for any other Degree or Diploma of any university or institution.

Date:

(Chandrajeet Yadav)

VIVA VOCE CERTIFICATE

This is to certify that the research work embodied in this thesis entitled **"Trusted Cloud Services Framework to Secure Cloud Computing",** in fulfilment of the requirement for award of degree of 'Doctor of Philosophy' in Computer Science & Engineering, of Maharishi University of Information Technology, Lucknow, Uttar Pradesh, has been approved after an oral examination of the same in collaboration with an external examiner.

Internal Examiner **External Examiner**

Deen Research

Date:

Place: Lucknow.

ACKNOWLEDGEMENT

First of all, I would like to thank the Almighty God for given me the strength and patience all through my journey in PhD research. This whole journey gives me lots of experience and makes me strong to fight any situation with patience and calmly.

I am very thankful and want to express my sincere gratitude to my respected supervisor **Dr. B.D.K. Patro** and Co-supervisor **Dr. Vikash Yadav** for their valuable guidance, keep interest, constructive counselling and critical appreciation throughout the course of present investigation. I am thankful to ALMIGHTY for providing me a mentor like them.

I convey my deepest gratitude to **Prof. Bhanu Pratap Singh**, Vice Chancellor, Maharishi University of Information Technology, Lucknow for providing the necessary facilities to work. Sir, I am very thankful to you constant support, encouragement and supreme guidance.

I would also extend my deepest gratitude towards **Prof. Akhand Pratap Singh**, Registrar, Maharishi University of Information Technology, Lucknow, for being an excellent administrator and teacher.

I also express my gratitude to **Mr. Girish Chhimwal**, Deputy Registrar, Maharishi University of Information Technology, Lucknow, whose affectionate behaviour has supported me through the course of this investigation.

I also express my gratitude to **Dr. Anil Kumar Dixit**, Dean Research, Maharishi University of Information Technology, Lucknow, for always extending his unconditional support and encouragement during my journey of doctoral research.

Mostly important, none of this would have been possible without the love and patience of my family. I can't image my current position without the love and support from my family. I very much thank my parents, **Mr. Shiv Kumar Yadav** and **Mrs. Svaroopa Devi** for striving hard to provide a good education for me and my sibling, Parents being external God who shaped my life deserve much more than what I can ever thank. Their silent prayers, aesthetic love and affection, support and firm belief in my capabilities have enabled me to take this Endeavour a success.

I always fall short of words and felt impossible to describe their support in words. If I have to mention one thing about them, among many, then I would proudly mention that my parents are very simple and they taught me how to lead a simple life. My family, to whom this thesis is dedicated to, has been a constant source of love, concern, support and strength all these years.

(Chandrajeet Yadav)

Date:

TABLE OF CONTENTS

REVIEW OF LITERATURE

CHAPTER I

INTRODUCTION

1.1 Overview

Over the internet cloud computing is termed as the services of computing delivery. In today's world, the majority of the people make use of cloud computing services for their personal needs. Modern-day software companies are in requirement of secure, fast, and scalable IT infrastructure, for the sake totally with the ever-growing demands of the business world. But, the challenge here depends on the setting up of this configuration in their personal areas. To supervise, a large disbursement is incurred against the developing requirements of the IT foundation, manpower and the proficiency. Thus, the goal is moved from their core business towards risk handling. As clouds represent a heterogeneous distributed systems and large-scale complex, resource management becomes a challenging task. As they assume this as a complex method, they hang on to an automated and combined brilliant strategy for utilizing the resources to supply services which is reliable, protective and efficient of cost. Hence, the necessity in platforms of software that represents the Clouds computing fabric is shown [1].

1.2 Fundamental Characteristics of Cloud Computing Technology

The five characteristics of cloud computing technology by NIST [2].

(i) On-demand self-service: A user can provide a sovereign provision of the efficiency of computing i.e. resources of the cloud must be available every time and the client firm should be able to access their resources of the cloud without providing the company's interaction.

(ii) Broad network access: Cloud computing is based on the network and used from anywhere and from any standardized platform (i.e. mobile devices, desktop computers etc.)

which means the capabilities are contained over the network and clients can access virtual servers and make use of their resources.

(iii)Resource pooling: The resources are shared in the cloud and meanwhile, the users may use the same set of resources. So, to avoid the capital outlay the provider follows the pay-as-go policy and provides the computing resources to many consumers.

(iv) Rapid elasticity: The response of the cloud is very quick and it can maintain a huge memory like an elastic structure. In some cases, the reactive time automatically alters to quickly scale out and quickly released to quickly scale in.

(v) Services measured: The cloud supplier must maintain and improvise the resource in terms of utilization of electricity and measures the amount of service provided and responds accordingly (both in terms of updating and software and hardware billing the client as appropriate).

1.3 Cloud Computing Architecture

Architecture of Cloud computing derives both the components that is used as well as its current working. Cloud computing consists of two components namely, the front end and the back end. The client part of the cloud computing system is present in the front end. It is composed of interfaces and the applications that is needed todeal the platform of cloud computing [3].

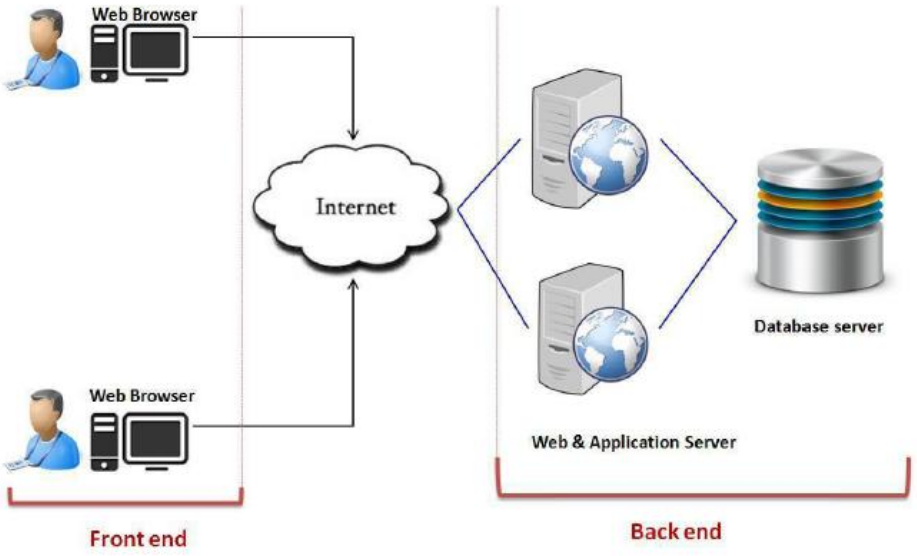


Figure 1.1: Cloud Computing Architecture

And the back end refers to the cloud itself, it contains the resources that are efficient for the services of cloud computing. It is composed of servers, virtual machines, data storage and security mechanisms etc. and it is maintained by the provider. The system of the file which is shared over any number of disk drives and machines is shipped by Cloud computing. The data is not stored in one specific location and other will take over by itself when case of one unit gets collapsed. Among the distributed system file, the disk space of the user is allotted while the algorithm utilized for allocation of resources is another major component under consideration. Cloud computing almost depends on an algorithm which is basically strong and it is considered as a firm distributed environment [4].

Cloud computing "implies to the applications that are provided as services through the Internet, and the system hardware and software models in the data centres helps to offer those services". Armbrust et al., presented "a utility oriented distributed computing system that contains a collection of inter-connected and virtualized computers that are dynamically deployed. Based on the service-level agreements created through negotiation between the service provider and the consumers are presented as one or more merged computing

resource(s)". Buyya et al. definition relates to the original flavour of this present evolution in distributed systems. From the private distributed systems, both the computing infrastructures and the applications of the software are carried out of various resources and the data centres of the third parties environment and access is made via the Internet.

As services based on subscription in a pay-as-you-go model, the cloud computing offers infrastructure, platform and software (applications). Now, within the industrial environment, subscription services are defined as IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service) correspondingly. To assist the end user applications globally the service providers like Amazon, HP, and IBM laboured Cloud data centres. From the common text processing software to online healthcare is the range of the applications. Users can access the cloud from desktops to smart phones, at anywhere and at any time by any gadgets once the applications are presented on the platforms of the cloud [5].

On the back end the system of the cloud knocks into the power of processing of the digital computers. It considerably quickens the speed of the application, which programs to pay for the services that are consumed by the user. Nevertheless, managing their liable elastic Cloud and reliable infrastructure that offers a secure, reliable and cost-efficient service becomes a demanding mission. At multiple layers, it requires co- enhancement (infrastructure, platform and application) thereby displaying the properties of autonomy. A system that provides computing power is said to be cloud Computing (Network , CPU, Random Access Memory, Operating System software storage, Speed) in the frame of a service through a web (normally on the internet) rather than maintaining physical computing resources at consumer's place.

Examples: Azure, AWS, Google Cloud

The word “Cloud” was originated from a model of the network that was used by the network engineers to display the place of several devices of the network and their interrelationship. Moreover, the form of the design of the network was almost like a cloud [6].

Cloud computing indicates to an alternate way for the whole combination of computer hardware and software that we use. So that, we can just sit before the desktop or somewhere inside our company's network and make use of this as a service offered by another company and can access the cloud through Internet. Basically, this is done in a stable path. The working of exact location of the software and hardware never remains as a considerable matter. Internet explains everything that happens here is that the user is somewhere up in the unclear "cloud".

A buzzword that represents the concept of‘different combination of services for the people who offers for a wide variety of services’ is insisted as Cloud computing. Few people compared this cloud computing technique with the Information technology offered services and view this as another method of IT based services implementation [7].

1.4 Problem Statement

The term Cloud Computing describes the metamorphic development of many existing technologies and handles computing at it is most basic, divides information and application resources from the basic infrastructure and mechanism used to deliver them with the addition of resources allocation with elasticity and utility model. Cloud Computing amplifies availability, collaboration, scale, agility and gives the potential for reduction of cost for the users and companies. In other words, Cloud Computing explains the use of application collections, information and infrastructure, network, information and storage resources and distributed services. These components can be organized fastly, equipped, implemented and disassembled using a utility model for allocation, de-allocation and consumption [8].

1.5 Necessity of Cloud Computing

Due to the increase of computer and Mobile user's, in all corresponding fields data storage has become a major concern. Many large and small scale businesses nowadays are growing rapidly towards the data of them. Furthermore, they are spending a large amount of expenses in maintaining the data. This successively trust on a very rigid help of IT and storage point. Every business could not afford this great expenditure sustained on the in-house infrastructure of IT and support of back up services. The cost effective solution for them is seen as cloud computing. Maybe its capability and effectiveness in the computational area, data storage, and less maintenance cost has made this technique attractive even for the large scale businesses [9].

By incorporating this method of Cloud computing, the user's need for the hardware and software combinational models which is considerably minimized. The user must be proficient to operate the cloud computing and that is the single thing offered by the consumer side, which should be simple as that of browsing the Web. The cloud network handles the balance matters, at some moment of time and an interesting insight are that what we experience in cloud computing. Some of the cloud services that are commonly known are mail services like Gmail, Hotmail or yahoo etc.

Our data is essentially stored on the server of the cloud and not on our PC's when using on E-mail services. The technology and infrastructure which is the backbone of the cloud is unseen. It is considered to the minimum as by which the cloud services are based on XML (extensible mark-up language), HTTP (Hypertext transfer protocol), Ruby, PHP or other corresponding languages moreover it is easy to use and functional. The cloud system can be accessed by the cloud user by their personal devices like desktop, mobile or laptop.

Cloud computing holds the skills of perfectly managing micro level businesses by means of possessing some amount of resources; it provides a technological access to small companies the technology that was out of range already [10].

Cloud computing allows small level businesses to transfer cost of maintaining their business into profits. We have to pay lot of attention to the in-house IT server to make sure that there are no errors in the system such that it works finely. We are completely responsible in case of any technical bugs. Thus it proves that a lot of focus is needed for an effective and efficient operation of the system without any flaws. Thus we can fix that both time and money is to be invested in excess for a high success. In cloud computing, the service provider is completely responsible for the complications issues and the technical faults that arise.

1.6 Working Models of Cloud Computing

There exist few models and services that effectively work behind to make the cloud computing services more feasible and accessible to the end users [11]. The working models of Cloud computing are as follows:

1.6.1 Deployment Model

1.6.2 Service Model

1.6.1 Deployment Model

The Deployment model addresses the kinds of approaches to the cloud, i.e., it indicates out the correct exact position of the cloud. There are four types of approaches in Cloud and it can choose any one among them accordingly: The approaches are as follows: The Public cloud, The Private, The Hybrid cloud, and The Community cloud.

1.6.1.1 Public Cloud

There are few systems and services available which can be easily approached by the people, this is the possibility that is implemented by the public cloud approach. The security feature of this approach is still a matter of concern and the contents of this cloud remains open to the public in which every user can access it.

1.6.1.2 Private Cloud

Whenever the systems and services offer a local approach, i.e. identical to those that can be deals with only inside a particular area or an organization, so that it comes under the private cloud category. It is considered to be safe and the contents always remain private.

1.6.1.3 Community Cloud

Only by a specific group of organizations, the services and systems remain accessible, then this method comes under the category of the community cloud.

1.6.1.4 Hybrid Cloud

The combination of the public and the private cloud is called as the hybrid cloud. The critical actions are handled by the private cloud while then on-critical actions are handled by the public cloud.

1.6.2 Service Model

Cloud computing depends on the following service models. Based on their needs, different businesses make use some or all of these components.

1.6.2.1 Software as a Service (SaaS)

1.6.2.2 Platform as a Service (PaaS)

1.6.2.3 Infrastructure as a Service (IaaS)

1.6.2.4 Anything-as-a-Service (XaaS)

1.6.2.1 Software as a Service (SaaS)

Software as a Service model makes use of the whole application that is operating on a system which is unknown. The best-known examples are Web-based email and Google Documents. Zoho is the best known SaaS provider which enables the functionality of many online applications that are exclusively withdrawn for office requirements.

Through internet this service becomes available to the consumers throughout the world. The software applications have to be purchased directly &then embedded in our computers. On the other hand SaaS users, instead of purchasing the software, subscribe is done by the users, usually on a monthly basis through the internet. Anyone in requirement of a specific fragment of software can subscribe this as a user, regardless of the number of employees in an organization. Software as a Service is considered consistent with all the devices in which there is an internet connection. Many jobs like accounting, invoicing, sales, and planning can be functioned with the help of SaaS.

Software as a Service (SaaS) is a method of cloud computing, which is seen as a delivery model of a software [12]. Software and associated data of it is handled at the core ((Internet) typically in the cloud) and can be approached easily by the consumers who uses a thin client model, generally using a web browser via the Internet. Customers are not awaited to purchase licenses of the software or infrastructure in related tools, and they are expected for paying monthly fees alone(also said as payments of annuity) .The utility charge is fixed according to their usage.

1.6.2.2 Platform as a Service (PaaS)

Platform as a service offers a platform and environment to permit the developers to develop services and applications. Thus, this service is hosted in the cloud and approached by the consumers through internet. To understand this with ease, let's compare this with the process of picture painting, where we would be provided with paint colours. Variety of paint brushes and paper and a beautiful picture must be drawn by us using such tools. The services of PaaS are updated in regular and continuously new characteristics are added.

The benefits of PaaS are enjoyed by the developers in Software, web developers and people in business. In order to support an application development, a platform is provided. It includes software support and management services, collaborating, networking, storage, deploying, testing, hosting and managing the applications. Cloud computing was developed to incorporate platforms for establishing and running applications of custom relations using the concept known as "Platform as a Service" (or PaaS).The next level is the PaaS, in which the required delivery is not an unusual thing of the software required, but it is said to be the users' platform. The whole infrastructure that is necessary to run the applications is delivered by PaaS through the Internet. Users can normally "tap in" and access the necessary data and complexities get restricted behind the scenes. PaaS depends on a model of metering or subscription. In such, the users only pay for utilizing and the delivery route in this PaaS model is the 'Cloud' [13].Platform as a Service (PaaS) model compares to the construction of the applications by making use of the Web-based tools which operate on an unknown company's software and hardware systems neatly. Construction of own ecommerce website that contains the features of shopping cart, checkouts, and payment option utilities are some of the suitable example for PaaS.

1.6.2.3 Infrastructure as a Service (IaaS)

Infrastructure as a Service model is known as one of the primary service models of cloud computing besides PaaS (Platform as a Service) model. It provides computing infrastructures such as network connections, virtual server space, bandwidth, load balancers and addresses of IP. This also provides redundancy and reliability to IaaS (Infrastructure as a Service), IaaS (Infrastructure as a service) model is seen as a complete package for computing. IaaS is one of the resolutions for small industries who are seeking for low expenses in IT infrastructure. Each year a large expenditure is acquired in the areas of maintenance and purchasing new components like network connections, hard-drives and external storage device, which the owner of the business can essentially store for other expenditures by using IaaS [14].

Infrastructure as a Service (IaaS) compares to the purchase of computing hardware devices which is used for many computational purposes namely the servers, drivers etc., through internet. We usually pay only for those devices that we purchase. Hence, the payment here is done based on our purchase which is also known as the utility computing method. Web hosting can indicated as a simple example of IaaS.

1.6.2.4 Anything-as-a-Service (XaaS)

This model is one of the model that is composed of Business-as-a-Service, Identity-as-a-Service, Network-as-a-Service, Database-as-a-Service or Strategy-as-a-Service.

1.7 Cloud Computing Features

Cloud computing is a technique which is Easily Manageable, where in the applications that we make use of something such that is issued by an unknown node that would never declare for ownership, which possess the ownership of that application completely. If we're using Google Documents, we need not worry about the purchase of umpteen licenses for the word-

processing software or about maintaining. Google takes care of the whole process and fulfils all the requirements. As far as cloud computing method is concerned we have to concentrate on the job that is allotted to us and need not bother about the features or services that is to be provided and it would be efficiently done by an outsider [15].

1.7.1 On-Demand Service

Cloud services are provided on on-demand and are often purchased on a "pay-as-you go" basis or based on subscription. We can purchase cloud computing in the same way as we purchase for electricity, telephone services, or Internet access from a company of utility. Cloud computing services can be purchased as per our requirement, which is same as that of the purchase of electricity, which is usually bought or paid for based on our consumptions. This feature makes the use of cloud computing technique more appropriate, as our needs changes accordingly.

1.7.2 Public or private Cloud

Nowadays the use of Personal computers has increased rapidly and the users have acquired the knowledge of both controlling and programming them as per our needs. At the same time, we have to remember that we are responsible for the outputs obtained. Any one of the two models cloud computing provides a resolution for all the issues encountered by incorporating, specifically the public and private models. The well-known example of a public cloud model is Web-based email. Private cloud computing system performs higher or lower in the same method similar to the public cloud computing system but the differences we can access the resources that we make use of via a much secure connection of network, mainly like an Intranet [16].

1.8 Schematic for Cloud Management

As the aim is to develop the management techniques and autonomic resource provisioning for assisting the applications of SaaS presented on Clouds, the following situations were identified:

1.8.1 Problems of Cloud Computing

Absence of control – The entire infrastructure of IT is deployed by its own to the third party externally. The question is how the business people manage a control towards their data and this is definitely overwhelming, which rests far apart the border.

Security – Over the year upcoming, protection of cloud computing environments would be a maximum consideration for the exertions of vendor's, said by(an analyst at Forrester Research)named Jonathan Penn. In less time interval, he witnessed users to perform a lot of base work, but after a while, "cloud providers should be aware of the opportunities provided to differentiate themselves by relating security". But institutions such as the (CSA) Cloud Security Alliance are now struggling hard for implementing suitable safety methods and the paths to present the same [17].

Security concerns – How business guarantees the user's secrecy and how the information is sustained during the usage of cloud? Data Integrity – While using of the third parties solutions for Cloud Computing what is the guarantee provided by the businesses for their useful information rests integral?

Availability –For enabling them to function effectively, the solutions of cloud computing rely mainly on the presence of their skeleton and the required customers applications of business. Just imagine a scene in which a Solution of a business critical Cloud remains unseen for certain time, then what will be its consequences on business?

Tolerability – How assured a business might be, if their third party solution is corresponding for its planned use.

1.9 Computing Security of the Cloud

Several sets of ideas and steps are incorporated in protecting data, its respective implementations and constructions. It is believed as a computer securities sub-domain.

1.9.1 Safety Issues in Cloud Computing

To protect the data and to maintain the processing power cloud computing and storage is enabled. Various service models are deployed by different organizations to relish the advantages of the cloud. Cloud computing grades the feature of authentication and it is explained as follows: encountering of authentication problems by cloud providers and authentication encountered by their consumers.

In Data authentication at the client side, the applications and the structural features turns out to be objective of the user in a cloud computing environment, so here comes the need for the user to design strong usernames and passwords.

In order to ensure data authentication, the approach to a server that is responsible for posting contents is lost, then gradually the system loses its capacity to protect the data that is considered personal from intra attacks. According to the recent Report of Cloud Security Alliance, attacks insider are considered as the sixth largest risk in cloud computing.[18]

1.9.2 Security Threats

Data breaches traditional corporate environments face many threats on the data stored, such threats mostly point on data tapping. At the same time cloud environments also suffer from the similar issues, as the data volume stored in this environment looks massive the cloud

providers become the capable objective of a hacker. To ensure right protection of data authentication, measures should be taken highly relies on the sensibility of the information that is to be protected, here the data attack and damage depends on the sensitivity level of the information. Data ruptures tells about damage on the data without regard to the type of information that it take over, here the chances of showing information's related to finance, health secrets and property rights looks to be utmost high [19].

1.9.3Oppressed system vulnerabilities

After the arrival of multi tenancy many old errors in cloud computing seems simple earlier and now it turned complex. Organizations pretend to distribute the memory databases and other resources in close adjacency among each another and generate new attack planes. Threats in a system can be identified and specific actions are taken out regularly, the system should be screened step by step in any case of flaws and this helps in over whelm effectively. Issues on a system can happen at any time rather than on predefined duration of time, once this faces action to alleviate the similar must be applied suddenly and regular updates on the up comings should be informed to the controlling head.

1.9.5Malicious insiders

Some attacks can be faced within a company; the attackers might be an employee who is currently working or the person who was formerly working in that company. And, if an account related to the business is hacked, then the attacker can be another partner of the respective company. Thus these are said to be different roles of the inside threats. The company can overtake these issues by easily retaining the whole control of the process of encryption itself; it also reduces the accessing authorities related to the user, thereby applying a control on unwanted approaches. While transferring the sensitive data there must be a

separate care among each zone. Therefore, proper training must be given to the administrators in order to correct respective mistakes [20].

1.9.5 Cloud service abuses

The chance of an abuse becomes maximum whenever an encryption keys opened. The attack can be carried out by capturing the cloud services and compelling them to support those atrocious performances. The cloud computing environment is bound to several types of attacks. In order to detect the type of abuse that the cloud computing system might clash, brief analysis should be done on several possible attacks and this is possible by thoroughly scanning the traffic. Observation of traffic may expose the presence of a special type of attack known as DDOs attack. This attack is considered to be harmful in nature hence corresponding preventive measures should be taken to escape from the consequences. Or else appropriate measures can be taken by the consumers to scan the traffic accurately and predict its consequences in advance such that respective preventive measures can be integrated [21].

1.9.6DoS attacks

When the mechanism of accessing turn out to be critical then it denotes the DoS type of attack. This type of attack is usual and it is found from the beginning of the strategies of encryption invasion. Whenever we struck in a heavy traffic, the only choice is to follow the vehicle in front or to simply remain patient till it gets clear and we have no other choices to either swing around or fly across. The similar thing happens in this attack, once it encounters we have no way to turn around, the only solution is to wait for its entire destruction. Another disadvantage is the overuse of power consumption. Finally the consumers are responsible and pay for the consumptions.

1.10 Cloud Security Controls

The stability of a standard Cloud security architecture is ensured by the proper implementation of several mechanisms of protection alone. Capable cloud security architecture must be in a location to find the issues arises with the management of security strategies. The issue is incorporated by the security management strategy with perfect security check.

The exposure of a system and its based abuses can be strengthened only if the possible controls are situated at the prescribed positions and triggered whenever needed. Cloud's structural security is dependent on various problems, specifically its controls helps more towards its stability and protection. Few noticeable controls that ensure the above mentioned features [22] are represented as follows.

1.10.1 Deterrent controls

A system of system cloud is always themed to various types of abuses; the main goal of any control is to reduce the effect of such abuses. Deterrent control is a control that analyses, observes, and enforces various steps in order to decrease the effect of that abuse on a cloud system. It is almost like a warning sign located on a fence or property; deterrent control reduces the level of threat by notifying the potential attackers about the unfavourable consequences if they continue they have to face the adverse effects.

1.10.2 Preventive controls

Preventive controls basically makes the system strong against adverse incidents, generally by means of reducing them or else actually stopping out such frailties. Extreme objective of any unauthorized user is by approaching the cloud. Preventive controls are used to raise the protection of vulnerable areas making it hard for any third person to use the same; this makes

the users of the cloud happy and enables them to feel strong enough to face any type of attacking problems.

1.10.2 Detective controls

The cloud system becomes weak once it faced an attack. In order to overcome this issues a perfect control method has to be used, to resolve this issue efficiently, the detective control method is found. It decides and implements the paths of finding and reacting to such unexpected violations. Let us assume a situation where a cloud system is on violation, in this type the detective control technique enforces steps compared to either its prevention or correction. A common problem in cloud systems is the Intruder's problem, to overcome this issue; we need to add extra security methods inside the system. This would indulge in permanent observation of security, enabling the features of both identification of invasion and its related precautionary action, thus makes the cloud more consistent in terms of authorized communications [23].

1.10.3 Corrective controls

Corrective controls reduces the harmful effects of an accident, basically by reducing the damages incurred. Either during or after the occurrence of an incident it is considered.

1.11 THREATS AND VULNERABILITIES OF CLOUD COMPUTING

1.11.1 Threats:

Rather than the security, system of cloud computing increases the consumer risks. CSA [24] and other organisations [25] has found the top main threats:

(i) Abuse and atrocious usage of cloud computing.

(ii) Insecurity of interfaces and application programming interfaces (API).

(iii) Vicious insider.

(iv) Issues of shared technology.

(v) Loss of data or leakage.

(vi) Account or hijacking of service

(vii) Unfamiliar risk profile.

These founded threats are descriptive of all the conceivable risks which may occur in the cloud. However, these threats derive the need of security. It would be difficult to build any services of cloud without security of cloud.

1.11.2 Vulnerabilities:

These are the following vulnerabilities [26] of cloud computing that is to be addressed:

(i) Authorization, system accountant, poor authentication.

(ii) De-provisioning and user provisioning; the customer ability to process control.

(iii) Remote access to the interface of the management.

(iv) Hypervisor vulnerabilities like virtual machine based root kit.

(v) Insufficient key encryption.

(vi) Insufficient standard solutions and technologies.

(vii) Management of poor key procedures.

(viii) Incorrect patterning of resource allocation.

(ix) Mis-configuration.

(x) Shortage of control in the process of vulnerability assessment.

(xi) The possibilities of internal network inquiring in the cloud.

(xii) Service level agreements with excessive business complications, clashing promises to stakeholders.

(xiii) Co-residency checks occurring possibilities.

(xiv) Inadequate certification or audit portion of cloud service provider.

(xv) The insufficient forensic readiness of sensitive data.

1.12 Encryption Algorithm of Cloud security

Few well-developed encryption algorithms which have been combined into the technique of cloud computing maximizes the secrecy protection. When the encryption data need process is nullified then this technique would essentially eliminate the keys and thus quit the process.

1.12.1 Cipher text-policy ABE (CP-ABE)

In the CP-ABE, the entire access strategy is controlled by the person who performs the process of encryption, as the strategy gets harder, the system design public key turns out to be much more difficult, and the system's security residue as the area of biggest concern. Points of access are hoped as required points as computations held at these zones. Hence a strong design model is needed to make these points strong enough to battle vulnerabilities; therefore structural stability is aimed by this method [27].

1.12.2 Key-policy ABE (KP-ABE)

This technique is comprised of encryption and decryption process. This method relies strongly on the incorporation of sets of attribute in order to explain about the cipher texts.

Encryption process is performed individually by merging the private keys with the text that is meant to be encrypted. Moreover the process of decryption is done by the user by them self.

1.12.3 Fully Holomorphic Encryption (FHE)

The objective of FHE is the direct computation of the cipher text that is said to be the data of encryption; any mathematical operation can be done directly on the data of encryption even before the decryption process, where the cipher text is converted to a plain text.

1.12.4 Searchable Encryption (SE)

The objective of SE if the function of identification that is to be enforced on the encrypted data in order to find potential risks with corresponding mechanism of authentication. The queries of the user can remain insecure in which these nodes are the possibility targets. Therefore, developing keyword indexes are safe that would provide the required protection and also supports in maximizing the need of identifying abuses or threats [28].

1.13 Current Trends in Cloud Computing

1.13.1 Composition of Definitions

One important word of caution is appeared: how we measure and forecast something as vague as "the cloud" trust on how we define it: if the definition goes on expanding, then perhaps that swings around to be the reason for the expansion of market as well? Hotmail is seen as an example of cloud computing. Using "the cloud" as a liberal synonym for "the Web," then by expressing astonishment that it's developing rapidly seems tautologous at best, since we are aware of that the Web and Internet have grown easily by virtue of possessing numerous connected users and (especially more mobile) devices [29].

1.13.2 Business benefits

For adopting cloud Businesses have a powerful and more interesting reason. The main advantages to purchase resources of computation at any instant of time depending upon our requirements.

1.13.3 Mobilization

Cloud computing is the vast transfer from desktop computers to mobile devices, and for the purpose of processing it consumes less power. “Thin clients" or "network computers" are represented by smart phones, tablets and various other mobile devices, as they complete the task assigned to them by means of the servers by which they are connected through internet. Internet of Things exhibits which is a new trend shows rise in the number of devices that is connected [30].

1.14 Challenges in Cloud Computing

1.14.1 Key Challenges

1.14.1.1 Quality of Service (QoS)

In order to satisfy the requirements of QoS of Cloud service consumers (CSCs) the cloud service providers (CSPs) wants to make sure that needed quantity of resources are furnished in particular of budget constraints, response time, deadline. Any deviation leads to fine, thus these QoS requirements nurture to create the basis of SLAs (Service Level Agreements). As a result, CSPs (Cloud Service Providers) need to guarantee that these deviations are either stopped or reduced by provisioning the correct quantity of resources in a manner of time possibly [31].

1.14.1.2 Efficiency of Energy

It describes about the competent energy utilization in the infrastructure, there by controlling applications utilization of more resources than the usual requirement and also concentrates on decreasing of application's carbon footprint of cloud.

1.14.1.3 Security:

Attaining security properties like confidentiality (securing data without authorization), existence (preventing from nasty users making the application impossible get the applications to legitimate users), and reliability against Denial of Service (DoS) attacks. If there is an improvement in the users number it makes automated increment in the number of resources that is allotted to the application, and the DoS attack is said as the critical attack since in the sketch of dynamic resource furnishings. The rapid increment in traffic might be wrongs legalize demands if an individual attack is initiated against the SaaS provider, and to handle them the resources would be mounted up. While executing the application this function would result in expenditure of cost (as the provider would charge for these extra resources usage) and loss of energy would be witnessed [32].

1.14.2 Cloud Testing Challenges

1.14.2.1 Non-Functional Testing

It is essential for the businesses and the provider who gives solution of the cloud to receive a precise knowledge about the needs within that business context before picking a resolution of computing the cloud. The business must carefully verify and do the requirement documentation with clarity and distinct. The primary key for the victory of any solution of the software is satisfying the requirements of business as it lays the principle for the delivery and the requirement is that it must be firm. Absolute testing on utilities of business will assure

that these are definite and perfect. This understanding of the necessities can be obtained from reviews, periodical gatherings of customer and workshops. This method accurately supports in time management and money; this would assist in the development of the software lifecycle by deleting the potential software mistakes before built-in. Necessary volume of testing is required in which scalability is considered as another major area of interest.

1.14.2.2 Functional Testing

In order to check its amenability needs, the process of testing all the parameters and system operation which comprises of the software, hardware and it is performed on an entire, system of incorporated software. In this script, is there any route and means by which such businesses approve and the system will cooperate within the specific requirements of the system? The method of testing the system enables the user in ensuring the attitude of the systems within its entity which is personal. It is necessary to witness that the system operates in the way it is designed and that the components of a system work in a united manner formerly, in any methods of functional employment. Expected inputs and outputs are obtained and the final solution system changes to be a productive system [33].

1.15 Advantages and Disadvantages of Cloud Computing

1.15.1 Advantages of Cloud Computing

Cloud computing technique stay obvious and forceful. Cloud computing permits for the purchase of services when required and thereby allowing us to increase the amount spent on unnecessary purchases when unwanted. We can prevent equipment going outmoded and other well-known problems related to IT like affirming safety of the system and reliability. When an extra need is arouse, we can notice suddenly by mentioning the need and hence obtain the requirements at the right instant. Appending raw applications to our jobs which is

existing happens at an instant of time and never takes weeks or months, thereby making it as a timesaving model.

Scalability –The primary advantage of cloud solutions is the on demand scaling. This can be accomplished through their distributed nature; this result in a distributed utilization that is even which can be approached easily by the servers which is present.

Location independent access –Concluded through virtualization or thin clients. The main disadvantage is it access through internet.

Ownership cost reduction –Skilled by utilizing the providers of the service with the presently alive detachments of the cloud and this would destructs the need to own hardware rather than providing support to the solution of the cloud.

Server efficiency/utilization –By consolidating the even distribution of workload the efficiency of the server and utilization has been improving greatly, thus it becomes feasible in achieving servers which is used less in which it generates the higher ROI.

Friendly with Infrastructure– The main aim of green computing is similar as that of the green chemistry; reducing the use of dangerous materials, achieving greater efficiency of energy throughout the lifetime of products, and promoting the biodegradability or recyclability of expired products and factory trashes. For business, the lower needs for implementations of hardware and depending on locations include benefits to the clean and pollution free environment. Now, there are number of researches who are in progress to play a role with a secure infrastructure of IT.

Instantly deployable environments – For specific efficiency like test or deployment, environments can be improved and utilized. Using the Cloud by the virtualization

requirement make sure that such environments become stretchable to the size of production and hence deployed within distant deadlines reduction.

Checks on cost maintenance– Based one single time, the focusing of every components of IT provides a vast influence on servicing that is taken out predominantly. The maintenance is thus duplicated in the instances of all the end user of cloud solution. With the list of advantages described above there are also a few matters which are to be reasoned by companies before adjusting themselves to Cloud Solutions [34].

The advantages of cloud computing are as follows:

1. Minimized IT infrastructure and computer expenses for consumers

2. Low maintenance issues

3. Better performance improvement

4. Instantaneous upgrades of the software

5. Improved and well recognized unity between the systems of operations

6. Outstanding restoration and backup

7. Functionality improvement

8. Excellent capacity of storage

9. Data security improvement

1.15.2 Disadvantages of Cloud Computing

Instant comfort arrives at a cost every time. For buying software or hardware models, cloud computing permits us to buy services, reducing the need, sometimes this seems costly. A

high-speed, highly reliable broadband Internet connection is always mandatory to make use of the software service model for the entire interval; hence the expenses of internet are controlled. That's an aspect that it is taken for granted in countries like the United States, at the same time it turns out to be a problem in rural areas or developing countries in which there is a less chances of broadband service connections [35].

Obviously Cloud computing provides pros in terms of comfort zone, yet there are boundaries farther the variations that we would like to incorporate.

• Easier in applications development.

• Mounted either up or down at a very short notice period.

• The expenses is only for the respective cloud usage alone.

• SLAS nurture to supervise all the incidents.

• Segmentation of complex systems is considered as another advantage of this technique.

1.16. Motivation

In this thesis, a new framework has been proposed and implemented in order to provide secured access for the cloud data using group key management techniques, Access Control Policies for cloud data and combination of access control and group key mechanisms for secured data access.

There are many contributions that have been made in this research work for ensuring the security of the data in cloud in communication. The major contributions are as follows.

To introduce an encryption model mainly to defence the data privacy. The proposed scheme along with the attributes is employed for data privacy and the identity of the user. The Advanced Encryption Standard (AES) is employed for data encryption.

- To minimise the computational overload the data file is accessed by the receiver corresponding to its weight.
- To propose a technique that reduces the communication cost, computation time and storage overhead in the cloud computing environment
- To provide a group communication in a secured way in the cloud environment using hierarchical group key management scheme.

1.17. Organization of thesis

The remainder of the thesis is organized as follows:

Chapter 2 presents a review of relevant literature carried out in this research work for securing the communication between the service provider and service user in cloud environment from various types of attacks.

Chapter 3 describes the overall framework of the proposed system in this thesis and also provides the mechanism to using group key management techniques for securing cloud environment.

Chapter 4 discusses a technique of access control technique for secured communication in cloud between the provider and the user in cloud.

Chapter 5 provides the conclusion on this work and suggests some possible future enhancements.

CHAPTER – 2

LITERATURE REVIEW

The chapter discusses various technical challenges associated with implementing cloud computing, as well as security concerns associated with cloud computing, particularly relating to data security, integrity, and authentication issues. In cloud environments, security issues such as worms, viruses, Denial of Service, password cracking, malware code injection, and scanning are common. Leaving these attacks unnoticed can harm the reputation of a company, as well as result in financial losses. This chapter presents a review and taxonomy, for the existing authentication and access control concerns from the perspective of the Cloud computing paradigm.

2.1 Introduction

As an emerging technology the cloud computing is established and it is used for many applications such as storage, data analysis and in Internet of things (IoT) [36-37]. The conventional approaches in the field of distributed computing handles the services using enterprises and cloud computing changes by offering various services to users. Most of these services are web-based services and no investment is required by the user in computing environment [38].

Some of the services provided by cloud computing are mentioned below:

• Infrastructure as a service (IaaS)

• Platform as a service (PaaS)

• Software as a service (SaaS)

A request must be submitted by the user in the above services to acquire the service from the service provider using the Internet and the resources are maintained and allocated by the service provider to accomplish the requests of the user [39, 40]. The resource allocation and scheduling algorithms are the service providers which manage the resources and schedule the incoming requests, so that the revenue could maximize by allocating resources. Scheduling and resource allocation are the main terms in a real-time environment adopting cloud computing [41, 42]. The National Institute of Standards and Technology (NIST) defines cloud computing as "a paradigm for facilitating on-demand, convenient network access to a shared pool of framed computing resources that can be provisioned rapidly and liberated with a nominal management effort or the contact of the service provider"[43]. There are five vital features in the cloud computing model presented by NIST, which comprise ample network access, resource pooling, rapid elasticity, on-demand self-service, and assessed service with four deployment models i.e. Private, Public, Community and Hybrid and three service models named as Software, Platform and Infrastructure. The above mentioned models are also identified as the SPI model. The most ingrained standard of these three SPI models is the IaaS which delivers a plentiful diversity of products and radical abilities such as on-demand provisioning, self-regulating scalability and pay-per-use [44-47]. Business shifting is done by several organizations over the cloud and the main reason is to develop their agenda at marginal cost and to achieve quick admission in outstanding business applications [48]. Several benefits are offered by the cloud such as metered services, rapid stationing, flexibility, scalability, pervasive network access, accelerated provisioning, prominent elasticity, data storage solutions, low-cost catastrophic restoration, rapid renovation of services, etc.[49].

In the cloud model, Flexibility and Multi-tenancy are the two key modules. Flexibility is the ability of the cloud for rising up and down the resources as current service demands and

among various tenants, sharing of same service instances are done by Multi-tenancy [50]. New users are concerned by these gains from industries and academies to guide the use of the cloud. Even though such services are provided by the cloud, it also offers many complications in adapting to these services. Many researchers in this particular context have focused their research which takes into consideration of security to various levels such as user authentication, data transmission, data storage, application, third party software, etc. Behind all services, cloud computing provides a shared and responsible security model.

The cloud consumer and provider have responsibilities in the security of cloud-delivered applications and the cloud-resident infrastructure. In each delivery model, the security requirements are different. For data security, the customer is responsible for some services like identity management and user access in any case of delivery models (IaaS, PaaS, and SaaS) as presented in Fig. 2. The security updates or patches before releasing, must be carefully verified, repacked and kept in the depository [51-53]. Regarding the system maintenance, the main role is for the customers like co-operating with the provider. Incidentally, the patches should be installed by them on the application stack and operating system (OS) moreover in the cloud framework the system administrator role should be performed by updating and patching the OS and several other applications [54].

Some other tasks of the customer are management of user account, destruction, and provisioning, password policies, authentication mechanisms of server-level accounts, etc. Using the logs the data activity of the customers can be automatically scrutinized and delivered to their accounts.

Though the cloud customer and provider are answerable for distinct aspects of the system and to protect the service they both must take some actions properly. Cloud Threat Report from the KPMG (2018) and Oracle and states that only 43% of suspects were able to spot the

security model of the IaaS. The network security panels should be employed by the establishments such as intrusion prevention and detection systems, physical and VM-based firewalls, gateways along with the determined workload, and cloud application controls [55-57].

A cyber-security incident reported that about 66% respondent's business operations were affected for the past 2 years. Some of these effects were interruption of service providing and business operation, delays in IT projects, and loss of employee productivity. Actually, a lot of attributions are provided by the cloud companies such as the provision of plenty of services, accessibility of powerful services, storing huge volumes of data [58].

2.2 Access Control and Data Authentication in Cloud Computing

In a cloud framework, access control ensures that only authorized users can access the data on the cloud server. Several malicious users or hackers may be trying to hack the data on the cloud server, which puts the security of the data at risk. During the last years, a lot of researches and implementations on authentication and security for limiting the risk of data loss and corruption had been performed.

Zhang et al. [59] presented the HGKA-OA protocol to enable privacy group communication in cloud computing systems. Different levels of privacy may be maintained while exchanging information among service users. To reach multi-level three-dimensional complex space security information exchange necessities, the author suggested a secret key factor combination technology. The protocol guaranteed that communication and computation are as easy and compact as feasible. Prediction of the protocol's security depends on the complexity of the DBDH and BDLP issues. The HGKA-OA protocol was also examined for security and efficiency, which suits multi-level and stereoscopic space security exchanging of information in cloud networking.

To obtain AKA among AVs, cloud and users in a CAV system Jiang et al. [60] introduced a cloud-centric 3FAKA protocol. To reach authentication on maintaining the privacy of their biometrics and identity, CT-AKA can meet three-factor authentication (i.e., biometric, smart card and password) by unifying three typical biometric privacy protection approaches, (i.e., fuzzy commitment, fuzzy extractor and fuzzy vault). Secure channels were established through both key agreement and mutual authentication to secure the communications among the cloud, from being maliciously controlled by attackers. This guaranteed strong security between the user and the cloud for information exchange that has also been demonstrated to be resistant to the breach of ephemeral security parameters.

A lightweight smart card-based remote authentication scheme was introduced by Sharma et al. [61] for cloud-based IoT applications. This scheme made use of the hash function and XOR. The scheme must be secure and robust to survive attacks because remote user authentication techniques are susceptible to adversarial assault. The quantity of big data exaggerates the Privacy and security concerns of cloud-based IoT. The suggested approach was not vulnerable to a user forgery threat. Automated Validation of Internet Security Protocols and Applications AVISPA was used to perform the legal security of the proposed scheme. With respect to computing cost, the proposed scheme's performance was compared to that of other relevant techniques. The comparison proved that the suggested method is more efficient than existing methods. In the authentication phases, login and registration, the suggested approach assumed computing costs of 9TH, 7TH and 6TH, and, respectively.

Extraction of features from three different traits by some unique image processing strategies was proposed by Joseph et al. [62]. In this paper, the performance of the XOR operation was done between the traits by converting the feature points into their binary equivalent. It was performed by iris and fingerprint data. The resulting binary vector performs XOR with the

binarized palm print feature vector. The resulting key was further converted into numbers and hash of strings using MD-5 hashing. Data encryption and decryption were performed by this generated secret key. The binary key size generated by MD-5 is normally 256 bits long. For data encryption, the first 56 bits of DES and the first 128 bits of AES and Blowfish are employed. This paper focused on maintaining high data privacy in the cloud networks. On comparing the three algorithms, AES obtained better privacy. Following that, Blowfish is considered, with DES taking the lowest position.

A Secure Sensor Cloud Architecture (SASC) was presented by Haseeb et al. [63] to improve the network flexibility with privacy and efficient data processing for IoT. They developed the architecture with two major phases. The one-time pad (OTP) encryption method, which protects the sensor-cloud infrastructure from unauthorized nodes, offered data security. It outperformed in terms of packet drop ratio, energy consumption, transmission overhead and network lifetime when compared to the existing architecture.

Xu et al. [64] suggested an enhanced RBAC approach based on an identity cryptosystem for cloud storage. With the use of a hybrid encryption policy and write-time re-encryption policy, this approach improved the encryption efficiency and performance of the system. Moreover, four tuples were used to represent the access control and the write-time re-encryption policy was used to improve the efficiency analyzed by the evolution method of Access control. Finally, Functional testing and performance analysis was evaluated finally which results in high efficiency.

To achieve effective CU revocation, data confidentiality and scalability Veerabathiran et al. [65] has introduced the CCDAC method. This approach was applied in the CCE risk ID stage that certifies a valuable, transparent and complete assessment of RF. In CCE, the scalability challenge was used to revoke CUs and ensure data confidentiality. This goal was achieved by

the use of HPRE as well as through the operations of AC and ENCP. The HPRE's uniqueness was based on the solution that determines the difference in encrypted D–JC data. As a result, it substantially reduces the computational difficulty of the CSP and cloud. Also, no additional link between cloud and CSP is required for the explanation. Finally, authentication and the computation model were specified and the absence of a CCE SECU threat evaluation was explored.

For a secured data access control optimization, a modified Chebyshev polynomial-based access control (MCPAC) was introduced by Benifa et al. [66]. MCPAC scheme was offered by verification and Authentications at various levels. This provided flexibility against well-known attacks. To evaluate the proposed access control scheme, the metrics such as detection rate, precision and recall are considered. This showed that the proposed scheme outperforms in terms of computational efficiency and satisfies the important security requirements. This makes it suitable for real-time applications mentioned in a cloud environment.

To use Swift in open source cloud was introduced by Anil Kumar et al. [67]. This was an object storage service known as Open Stack. Swift restricts to use of Access Control Lists (ACLs) objects. An object could be accessed by users who have access to it according to the ACL. However, once the user is allowed to access it, then the entire object was accessed without any restrictions. They proposed this new model to meet authentication and data integrity in an interacted and distributed environment. The facility to inter-operate among processes running on the diverse cloud providers and identity authentication was achieved by this model. This proposed method is implemented in a real cloud environment such as Microsoft Azure, Open stack and Amazon cloud. To provide compact access control to Swift storage, an agenda named Predicate Based Access Control (PBAC) was introduced. It shows

that, in the cross-cloud environment, a stable and reliable system can be built safely and efficiently.

Megouache et al. [68] designed an access control framework for an environment for cloud services. The conventional access control mechanism does not obtain the necessity of the cloud environment. Also in this paper, the author proposed an innovational and an attribute-based credit computational model. In this paper, the attribute-based access control was incorporated by the credit component module. The concept of crowd evaluation and sign was used to compute the user's credit value.

An ASBAC (Symbolic Attribute-Based Access Control) system was developed by Anil Kumar et al. [69] to secure the cloud environment. By utilizing the Message Digest-5 encryption algorithm, the SABAC system was developed using Hash-tag Symbol Authentication (HSA). Utilizing a system that uses a username and password, as well as an HSA code, and real-time image monitoring, SABAC implements a 3-Tier continuous authentication method. Using the obfuscation technique, the HSA code is generated by combining five-tuple user attributes and the image file. By converting the concatenated string to hexadecimal, the HSA code is created by integrating an MD5 algorithm. In order to evaluate SABAC, three metrics were used: availability, integrity and confidentiality. SABAC appears to be highly effective at protecting cloud data. Any fake identity would be impossible to match with valid HSA data in this database, so hackers could not match any of the fake identities to the databases. It showed that SABAC could guarantee data security in a cloud environment. It was suggested that the SABAC system be adopted by Cloud Solution Providers and Security Specialists.

In a multi-authority cloud, a secure, fine-grained and adaptable access control model was suggested by Fugkeaw et al. [70] for a large amount of data. To expand the process of a

policy update to the cloud server, they have designed VL-PRE (Very Lightweight Proxy Re-Encryption) scheme. In the cloud, communication cost and computation at both data owners and a proxy were optimized by VLPRE that dealt with file re-encryption and re-encryption key generation. An efficient policy updating algorithm was developed that meets accountability, correctness and security requirement. Thus, the deployment of our access control embedding the VL-PRE approach will eventually serve as a practical security application in the cyber-enabled big data cloud system.

Wang et al. [71] has developed an innovative access control model for IoT based on the ABAC model, supporting trust attribute called T-ABAC. ABAC was combined with TBAC representing as T-ABAC that deploys secured evaluation model in IoT system by more privacy requirements. Also, the complexity of traditional cross-domain mapping was avoided by attribute consistency between domains and the problem of cross-domain is transformed into the problem of distributed identity authentication. Additionally, to reduce the effect of subjective factors in trust evaluation the authors have proposed an integrated weighting method that ensures the objectivity and accuracy of the trust evaluation.

To contribute to resource consumption accounting the authors Xue et al. [72] has proposed a combination of data owner-side and cloud-side access control in an encrypted cloud environment, which is resistant to EDoS attacks. This system assisted arbitrary CP-ABE constructions. The structure is trustable from the harmful covert cloud providers and data users. We relax the security requirement of the cloud provider to covert adversaries, which is a more practical and relaxed notion than that with semi-honest adversaries. To limit the overhead of using covert security, the author introduced a bloom filter and a probabilistic check in the resource consumption accounting.

A new encryption scheme named, AES Lightweight CP-ABE was developed by Yadav et al. [73] to secure the privacy of data in the cloud environment. This proposed scheme has undergone double encryption on the cloud data. The Lightweight CP-ABE performed the initial encryption and the secondary encryption was executed by AES. The access control was assumed by the digital signature. In the cloud framework, the owner and the user obtain authentication. With definite question the attribute set was created, when the cloud user tries to access that randomly appears.

To maintain data security in addition to access control channel et al. [74] introduced a new encryption design called Attribute-based Encryption" (AES–CP–IDABE) and "Advanced Encryption Standard–Cipher-text-Identity. In this paper, along with the user's attributes and identify the data was double encrypted eventually using the ABE. Moreover, the encryption of data was done by using the Advanced Encryption Standard (AES) and made it available to authorized users. With the support of user ID and security keys, the digital signature was used to develop user access control. In addition to that, Denial-of-Service (DoS) detection setup was included by monitoring and controlling IP addresses. This scheme was evaluated in terms of performance between the user-data owner communication with the execution time of the user.

To ensure the proper control, integrity and confidentiality of access to sensitive data Mahmood et al. [75] has suggested access control and cryptography. They proposed this model for securing information in the cloud environment. To improve security and data access this model was built with a hybrid of a role-based access control model and a markup language for expandable access control (XACML) and an improved RSA encryption algorithm. This paper was suggested storing information in cloud environment with the use of

cryptography and along with the access control model it allows the data with limited time and encryption-decryption cost.

Eltayieb et al. [76] presented a scheme known as attribute-based secure data sharing (ASDS) for cloud computing, that allows data confidentiality, flexible user revocation, data authentication and data access control. Furthermore, the suggested scheme was resistant to replay and collusion attacks. On evaluating system security and the performance comparison with another data-sharing framework, attribute-based secure data sharing (ASDS) has been shown to be feasible for cloud users.

Li et al. [77] presented a mechanism for key updating and authenticator evolution for secure cloud data auditing and zero-knowledge privacy with zero-knowledge proofs, Homomorphic linear authenticators and proxy resignatures. The suggested method used the Shacham-Waters auditing scheme, which is the state-of-the-art approach. Cloud users can update their key without downloading the entire file and all the authenticators need to be regenerated, using the new private key, the user can create a re-signing key with one single file tag and the new file tag accompanied by verification information is uploaded to its cloud server in which updates are the phase where the user undergoes the least amount of work. Using this method, communication and computation costs are drastically reduced while maintaining desired security. The auditing scheme of key updating is formalized in the context of zero-knowledge data privacy and ensures that the proposed construction is sound and has zero-knowledge privacy. Implementing a prototype of the protocol demonstrates the viability of the proposal.

The authors Li et al. [78] has introduced a novel offline/online ABC method for removing most of the computation task by including system public parameters in addition to relocating the encryption computational complexity to the offline stage on the owner side of data. Before the decryption stage, a public cipher text test stage was conducted. This result in

removing the majority of the computational cost associated with unauthorized cipher texts. To be specific, the public cipher text test enables a user to determine how a potential equation can hold for components of a given cipher text at a reduced price. To generate an instantaneous cipher text, the Chameleon hash function approach is utilized that was blinded using offline cipher texts in order to access the final online cipher texts. In such manner, the suggested scheme has proven CCA2 secure that was widely accepted as a standard security concept.

Ding et al. [79] has designed PF-CPABE a new efficient CP-ABE access control technique for information sharing in IoT systems. In this paper, they exchanged simplified scalar multiplication on elliptic curves for complex bilinear pairing. As a result, the user's overall overhead was greatly reduced. To suspend a user's authorization directly or to modify an attribute without changing the keys of other users they also designed a new way of key distribution, so that the system can directly suspend a user's authorization. To obtain a variety of access control requirements in practical application this design made use of an expressive LSSS access structure.

To categorize clients into different categories depending on assigned attributes (like employee id, age, name etc...) and privileges, Challagidad et al. [80] has developed RHA. This category was essential in order to make efficient use of cloud services and permits the clients to access information within their own limit. RHA protects users from accessing data that is not intended for them. A hierarchy access structure (HAS) was built to allow numerous hierarchical files to be shared and address the multi-authority access control scheme collusion problem for cloud data storage. The suggested design was for preserving user data, ensuring privacy and access control with multi-authorization in cloud storage. An existing FH-CPABE was used to encrypt users' data or employee's data based upon defined access policies. It has

been established that when the number of authorities increases, the time consumed by Lewko's approach also increased when compared with the proposed scheme. Hence the suggested scheme gave effective multi-authority access control.

This ABE-FPP, with full privacy protection (FPP) a lightweight attribute-based scheme of access control (FPP), that achieves the whole protection of privacy was shown in the three key stages (i.e., partial decryption, generation of key and access control) and while decreasing the utilization of overhead on the user side was presented by Tian et al. [81] in this paper. In particular, a lightweight two-side safety computing protocol among the user and the authority is modeled to generate secret keys to protect privacy during the generation of the key, they introduced a capable strategy of hidden policy to protect privacy at the time of setting the access control policy. It only shows the attribute names and effectively hides the values of the attribute. They proposed a technique of hybrid authentication in order to protect privacy policy at the time of partial decryption that there is no necessity of submitting the values of the attribute to the cloud. Besides, for achieving the estimation of lightweight for the devices of IoT, the employment of encrypting the online/offline and decryption of outsourcing in ABE-FPP is done. At last, evidence of formal security exhibits that the scheme of us was secure in the ideal model.

To store information and secure key in cloud Xionget al. [82] has constructed a modern CP-ABE based storage model for IoT applications. This paper presented an attribute authority management (AAM) module within the system of cloud storage worked as a specialist that gives a convenient permission control and exceedingly limits the capacity overhead of public keys. At that point, they proposed an innovative effective and secure multi-authority access control method of the cloud storage framework for IoT, to be specific SEM-ACSIT that gets both in reverse security and forward security when an attribute of a client is denied. By

misusing encryption outsourcing, modified key structure and the AAM module, the computational overhead of a client is massively reduced. In addition, a client access control list (UACL) within the cloud server was newly built for a particular client to back authorization access.

For IoT systems, Ding et al. [83] has demonstrated new attribute-based access controls, eliminating the need for ACLs or roles for every user. The system can describe each device by a set of attributes that are predefined by the attribute authorities based on its identity or capability. No one can access the device until they have sufficient attributes that meet the access policy. In order to record attribute distribution, they used blockchains. A public and credible ledger of 'transactions' is maintained by the attributes authorities. Data in a Blockchain can never be altered after it has been recorded and can be accessed at any time by anyone who needs access. AKA protocol, consensus algorithm, and other parts of the proposed scheme are modular, which contributes greatly to the flexibility of the system and facilitates future maintenance and upgrades.

A novel key agreement scheme was presented by Yu et al. [84] for cloud computing based on IoT. Security verification was conducted using informal security analysis, BAN-logic verification and automated security verification (ProVerif) (ProVerif). It showed that the proposed scheme is secure, can effectively resist all kinds of attacks, and can be deployed quickly. Further, compared to the original scheme, the proposed scheme has proved superior security and performance characteristics.

Belguith et al. [85] proposed responsible protection protecting attribute-based system, called Ins-PAbAC that combined quality-based encryption and property-based signature procedures for safely sharing outsourced information substance by means of open cloud servers. The suggested system presents a few focal points. To begin with, it gave a scrambled get to

control include, upheld at the information owner's side, whereas giving the specified expressiveness of getting to control approaches. Moment, Ins-PAbAC jam users' protection, depending on a mysterious confirmation instrument, inferred from a security protecting quality-based signature conspire that covers up the users' recognizing data. Moreover, their proposition presents a responsible property-based signature that empowers a review specialist to uncover the personality of the anonymously authenticated client in the event that required. Third, Ins-PAbAC is provably secure, because it is safe to both inquisitive cloud suppliers and noxious client's foes.

The main issues related to cloud-based big data security were presented by Narayanan et al. [86] in this paper. Innovative system architecture called Secure Authentication and Data Sharing in Cloud (SADS-Cloud) was designed. This paper involves three processes, including (i) Big Data Management, (ii) Big Data Sharing and (iii) Big Data Outsourcing. SHA-3 hashing was used by Trust Centres to verify data owners in big data outsourcing. The input file is split into fixed-size data blocks using the Map Reduce model, followed by the SALSA20 algorithm applied to each block. Big data users receive files in a secure manner through big data sharing. Authentication was carried out by hashing the credentials (such as email id, current timestamp, secure ID, password and ID) and comparing them with those stored in the database. The Big data management process involves three crucial steps. The three algorithms are Compression via Lemperl Ziv Markow Algorithm (LZMA), Clustering via Density-based Clustering of Applications with Noise (DBSCAN) and Indexing via Fractal Index Tree.

The PMDAC-ABSC scheme is a novel privacy-preserving data access control scheme suggested by Xu et al. [87] that uses Cipher text-Policy ABSC to protect attribute privacy of information stored in a multi-authority cloud storage system by providing a fine-grained

control measure. Signcryptors as well as design crypto's can have their attributes protected to not be known to cloud users and authorities. Moreover, the cloud server's bilinear pairing operations are outsourced to the user, reducing the decryption overhead without degrading the attribute privacy.

A task planning algorithm for heterogeneous cloud computing systems has been proposed by Panda et al. [88] known as an energy-efficient task scheduling algorithm (ETSA). A proposed energy-efficient task scheduling algorithm (ETSA) is an online algorithm meant to integrate heterogeneous cloud computing systems. The algorithm requires maximum completion times, m resources and n different tasks. They evaluated ETSA for energy consumption and make span with various modified benchmarks and synthetic datasets.

2.3 Scheduling and Virtual Machine Allocation Based Techniques:

Additionally to resource reservation, Zhang et al. [89] has proposed a virtual machine allocation system. Energy consumption was determined by a fitness function. Based on the execution time, energy consumption, profit, and acceptance of applications, the mechanism is estimated according to VM capacity, entry time, and execution time. Evaluations are conducted in CloudSim as well as in a real-world environment.

Alhassan et al. [90] has demonstrated a Haizea algorithm to assign VMs for IaaS, and a greedy policy to choose servers. Each node was ranked based on its cost and capacity. Thereafter, the nodes are arranged and the suitable node is determined.

RMSE values of less than 2% were proposed by Bouterse et al. [91] for simple approximations. Specifically, it was shown that the distribution of the number of customers can be approximated well by the normal distribution N (ρ, ρ), where ρ is the offered traffic load. The number of in-service virtual machines in the system can be also approximated by N

(ρ + R, ρ). This is a very useful result, which allows the percentile to be computed easily for any given offered traffic load. Additionally, the utilization is shown to be dependent on R and ρ values, and the average utilization can be approximated by 1-R/(ρ + R), where R/(ρ + R) approximates the proportion of expected losses due to R. The queue length distribution of the number of waiting for customers is very small, and it was shown that the queue length distribution does not only depend on ρ as is the case of birth-death queues, but it also depends on the value of λ and μ. This unexpected result is due to the periodic adjustment of the capacity of the system.

An approach to provisioning virtual machines for cloud-based software used as a SaaS, where customers arrive periodically was described by Bouterse et al. [92] in this paper. The provision model depends on knowing the number of arrivals during a given inspection period. In order to accomplish this goal, they constructed and compared the following forecasting models: exponential moving average, moving average, autoregressive model, Autoregressive Hidden Markov model and mixed auto regressive model. The fixed reserve capacity model was also proposed, a simple strategy where, at the beginning of each inspection interval, the number of VMs required is adjusted up or down so that R seats are always available.

A prediction mechanism for Minimization of Migration (MM) policy was designed and implemented by Tarahomi et al. [93] mainly for the large historical data set, accompanied by a dynamic thresholding mechanism alongside static thresholds. According to the experimental estimation, the cloud data centre consumes less energy. The most significant feature of cloud servers is their efficiency in power consumption. Green computing is based on the efficient use of power. Data centre physical resources can be allocated to VMs using power-aware methods. Virtualization is a method of allocating VMs that is power-conscious.

The priority-based VM allocation scheme was designed by Son et al. [94] to correctly allocate bandwidth and path traffic based on the priority-based VM allocation scheme. A critical application can be appropriately supported even in a busy data centre by ensuring that the networking and computing resources are sufficient. Our critical application traffic utilizes a network bandwidth allocation strategy enabled by SDN, so that the application can complete transmission of network on time regardless of network conditions. The QoS-critical applications of our approach can be run in time on the cloud while other applications can still share those resources. To avoid network delays that can affect QoS, the host and networking resources are taken into account jointly. QoS requirements for the applications are implicitly provided to cloud management during the application request. In addition to calculating QoS requirements including bandwidth and computing capacity, the proposed algorithm identifies spots where VMs and flows can be connected. Computing and networking requirements are both taken into account when the algorithm is used to select a host for the VM and the links between hosts. They utilized dynamic bandwidth allocation to meet the requirement of networks after selecting the network links. In a multi-tenant cloud data centre, it is found that combining the proposed scheme can provide appropriate resources for superior applications to meet the requirements of QoS.

Considering both the host and the network resources, Hanini et al. [95] suggested the priority-aware VM allocation (PAVA) algorithm. They proposed placing the high-priority application's on VMs to reduce network congestion. With the support of SDN controllers, each networking device of a data centre network was configured with priority queues to guarantee the availability of the network bandwidth for critical applications. Based on the outcome of the research, the proposed approach in a multi-tenant data centre can allocate sufficient resources for high-priority applications to get the application's requirement of QoS.

Using the VM utilization method combined with a method for controlling the access requested to VM monitor, Saxena et al. [96] built an approach for maximizing VM utilization. VM activation is based on workload, while access control determines the number of requests. Detailed mathematical models were developed and evaluated for both the proposed approach and its performance parameters. This approach exhibits a positive impact on the results.

A model for allocating resources to tasks requested by different users was presented by Zhang et al. [97]. As a matter of fact, it can decrease providers' costs and enable users to complete tasks on time. In order to accelerate convergence and to avoid falling into local optima, they proposed a solution algorithm in which they presented new mutation strategies for the standard DE algorithm and crossover operations were performed. On comparing with the existing approach it showed that the proposed approach is faster than DE at convergent. It also indicates that it can produce resource allocation plans with a shorter duration than those achieved by other compared methods, including two representative methods, RR and min–min.

The Evolutionary Allocation and Consolidation of VMs among Heterogeneous PMs was proposed by Zhang et al. [98]. With this approach, they determined the optimal instruction-energy ratio of PMs so that they consume less energy. Additionally, to facilitate fast VM allocation evaluation, the search for optimal results leads to develop a coarse-grained simulation engine and adding it to CloudSim.

Rahmanian et al. [99] presented an algorithm for optimizing energy consumption at cloud data centres so that SLAs are not violated as well as host and switch consumption. Data centre architecture and component positions are taken into account by our algorithm. Consolidating VMs on the optimal sub-network of data centres will allow other network

elements such as switches to be turned off. Briefly, the algorithm depends on how efficiently the host uses energy and obtaining an energy-efficient sub-network and optimize the device's operation.

BB-BC optimization method was used to optimize the performance of the proposed scheme was implemented by Rawat et al. [100]. There exists a search space that includes all possible schedules using randomly generated populations and time and cost establish optimization parameters. A big bang theory is used in this approach. The algorithm can be configured by initializing some elementary parameters. A population count, cloud main resources, and a number of tasks assigned to each virtual machine are included. This task is performed in a random way by the virtual machine. Virtual machines with the best schedule were assigned tasks when the population size equals 100. With a random-based algorithm, 100 cloudlets were executed on five virtual machines. BB-BC-based optimization is found to be the best solution. Evolutionary techniques use the best fitness value to provide quality service. Cost and execution time affect fitness function.

To solve the problem of VM co-residency security, Jia et al. [101] proposed a VM allocation strategy (SC-PSSF) with energy-saving and load balancing as optimization objectives. Reduced CPU and numbers on the host resulted in energy savings. SC-PSSF has been proven to be more energy-efficient.

Qie et al. [102] presented an energy-efficient Virtual Machine (VM) allocation scheme that combines asynchronous multi-sleep with adaptive task migration. VMs that are part of a virtual cluster can be broken down into two modules, namely, Module I and Module II. In Module I, all the VMs are awake, but in Module II, the VMs will sleep independently if it is possible. The proposed strategy was captured by asynchronous multiple vacations queuing model based on a partial asynchronous queue. Matrix-geometric methods was used to

calculate performance metrics in terms of the average response time of tasks and the rate of energy savings of the system. Several numerical experiments are performed, employing analysis and simulation, in order to validate the proposed VM allocation strategy. Additionally, system parameters are assessed to estimate the influence of performance measures. Finally, they construct a system cost function to trade between different performance measures. Additionally, VMs in Module II was optimized by using an intelligent searching algorithm and also the sleeping parameter.

Wang et al. [103] designed a scheme for allocating VMs that is energy-saving while constrained by responsiveness in a cloud environment. A system's virtual machines, including the PM itself, stay awake during a period when there are no tasks yet present, rather than immediately switching into the sleep state. This allowed the newly arrived tasks to get serviced as soon as possible. Using this method, users' quality of life can be assured, additionally, there was a reduction in energy consumption. Using mathematical methods, they modelled the scheme and evaluated its performance. They proposed a method for running multi-server queues in cloud data centres in order to capture the stochastic behaviour of the tasks. Our system's efficiency can be evaluated by creating a two-dimensional Markov chain (MC) that provides an average latency measure and energy-saving analysis.

The cloud servers are interconnected in this work by a step network and Processor energy consumption model using UML, motherboard, electrical components, hard disk and dynamic random access memory was developed by Zaidi et al. [104]. This paper also discussed how to balance workload by mapping cloudlets to VMs and Workload allocation according to Round-robin policy. With this approach, tasks are bound to VM for high-speed execution or a short execution time. Data centre policies use service proximity to route user traffic to the nearest data centre with the lowest network delay. To design a class diagram, a well-known

Unified Modelling Language must be used. An analysis of response time and internet characteristics was carried out.

In the cloud computing platform, an ant colony optimization-based VM allocation method (VMA-ACO) was developed by Xu et al. [105] for load balancing multi-dimensional resources. This paper introduced a PM selection expectation concept to overcome basic ACO shortcomings. Based on its NP-hard feature, they devised an efficient virtual machine allocation algorithm based on the ant colony optimization algorithm. In particular, the ant colony optimization should be customized for virtual machine allocation and to prevent premature convergence of the basic ant colony optimization, improve the physical machine selection approach or a local optimum is reached.

Omer et al. [106] in this approach suggested that Power and network consumption must be minimized and CDC waste in a dimensional and heterogeneous environment. Specifically, our paper proposed a novel priority-aware VMP algorithm capable of optimizing the consumption of power, waste of resources, and network resource usage simultaneously in a multidimensional and heterogeneous CDC. Specifically, this paper developed a priority-aware VMP algorithm capable of optimizing the power consumption, waste of resources, and network resource usage simultaneously in a multidimensional and heterogeneous CDC. Two efficient heuristic algorithms were presented based on the priority level of IoT applications (normal or critical). An algorithm called a Joint Power and Traffic optimization algorithm (Joint PT) is presented for critical applications. A key goal of Joint PT is to maximize both energy efficiency and QoS is that by utilizing power-efficient PMs, for instance, would reduce the power consumption and placing mutual VMs with higher traffic demands on PMs in close proximity can reduce the network consumption. From Joint Power and Resource Optimization algorithm, Joint PR is presented for normal applications. The main goals of

Joint PR are to minimize total power consumption and resource wastage in CDCs by hosting each VM of a normal application on the power-efficient PM with the appropriate level of resources and with the least amount of resource wastage.

In order to resolve the SVP problem, 'Previously Co-Located Users First' was proposed by Agarwal et al. [107]. We used metrics to measure the resource efficiency and VM placement algorithms for security, including Core Utilization and Co-location Resistance. Additionally, cloud providers can utilize this algorithm to enforce security across multiple tenants in a public IaaS cloud. They compared the theoretical estimation of co-location resistance to the empirically obtained results using our algorithm. The proposed algorithm was thoroughly empirically tested against other widely used algorithms and a new trace of workloads from Microsoft Azure was used to build secure placement algorithms. Passive cache monitoring is investigated as a potential strategy for cloud users and VM placement algorithms can be improved by using binary classifiers.

A levy-based multi-objective gray wolf optimization (LMOGWO) algorithm was introduced by et al. [108] to provide an efficient solution to the VM placement problem. Pareto front data is stored and retrieved through an archive. They used a grid mechanism to enhance non-dominated VMs in the archive. An archive is also maintained using a mechanism. Grey wolves (GWs) are mimicked in a multi-objective search space by a proposed algorithm. Testing of the proposed algorithm was done on nine bi- and tri-objective benchmark functions to ensure compatibility. They compared LMOGWO with MOGWO and MOPSO. For the purpose of checking the adaptability of the proposed algorithm, two scenarios were taken for simulations. An LMOGWO tended to outperform MOGWO and MOPSO for University of Florida 1 (UF1), University of Florida 5, University of Florida 7 and University of Florida 8 for Scenario 1. Despite this, MOGWO and MOPSO performed well for UF2.On

Scenario 2, LMOGWO outperformed UF9, UF8, and UF5 compared to the other two algorithms. On the other hand, MOGWO performed well for UF4 and UF2.

Ponraj et al. [109] proposed a VMs placement algorithm based on computation time and logic complexity and in this manner, we can reduce the time it takes to complete the job overall. A VM placement algorithm has been implemented with both static and dynamic workloads. A simulation and analysis of the proposed algorithm were performed using Cloud Reports and Cloud Analyst. The key advantage of the proposed algorithm was that it reduced the performance cost of executing tasks submitted to virtual machines to the extent that the application can execute them and a reduction in processing costs is needed to achieve high performance. This algorithm optimizes the performance of cloud-based applications.

In this paper, Rani et al. [110] introduced ant colony optimization and gravitational search are combined into an algorithm to solve the load balancing issue. A hybrid approach has proven to be more effective than a basic approach. Ant colony optimization was avoided in favour of distributed search, which was lacking in gravitational search. CloudSim simulations show that the proposed algorithm improves task completion times using CloudSim when implemented as well as distributing virtual machine loads equally, this helps create a balance between virtual machine loads, by reducing resource consumption, they can reduce our environmental impact. Additionally, the hybrid algorithm can analyze the machine's capability and can assign tasks in an efficient manner, thus increasing the machines' efficiency.

CHAPTER III

AES- LIGHT WEIGHT CP–ABE BASED PRIVACY PROTECTION FRAMEWORK WITH EFFECTIVE ACCESS CONTROL MECHANISM IN CLOUD FRAMEWORK

In this chapter, we have proposed a novel encryption model named the "Advanced Encryption Standard with *Lightweight* Cipher-text-Identity and Attribute-based Encryption" (AES– Lightweight CP–ABE) mainly to defence the data privacy. Attaining the essential facts of the owner the owner-side authentication is provided. During the authentication process in the user-side two layers are provided for generating the attributes. For identity generation, the basic information of the user is employed along with certain demands, for ensuring the validity of the user. The AES cryptography is used to encrypt the data in the proposed model and the independent keys of the user is used to decrypt it effectively. The proposed model along with securing the data minimises the resource consumption and overhead. The proposed scheme along with the attributes is employed for data privacy and the identity of the user. The Advanced Encryption Standard (AES) is employed for data encryption.

3.1INTRODUCTION

Numerous adaptive computing resources such as servers, networks storages, and services are pooled to form the cloud computing that helps in offering appropriate and on-demand access to users in cloud [111]. Several commercial fields use cloud computing and also it is largely mentioned by people. The cloud service providers (CSPs) of the cloud framework are liable for equivalence and other administrational modules. The liabilities elicited in the identity management systems leads to an abundance of data leakage incidents [112]. The vital concern of the cloud framework is the Identity and access management (IAM) for the

approval of cloud-based services. Currently, the CSP are answerable for the identity management process, which barely experiences the constraint of a fine-grained and adaptable access control policy of the user. In cloud computing data confidentiality is not certain [113,114]. If data is stored in its original pattern any third party could possibly leak the personal data's. Therefore, the sensitive data of the data owners are not exposed and stored in the public cloud. Hence, in the public servers a new access control strategy is required. To achieve this, data encryption is done using many encryption methods. Data confidentiality is achieved using the access control through encryption and moreover the malicious users are banned from using the personal data from unauthorized access.

In mobile cloud environment to ensure confidentiality and access control a cryptographic method named the ABE is implemented [115-117].

Using fine-grained access policies the encrypted data of the user is stored by the data owner and the access privileges must be fulfil by the user to access a particular data.

Cipher text-policy attribute-based encryption (CP-ABE) and key-policy attribute-based encryption (KP-ABE) are the two types of ABE. A set of attributes in KP-ABE [118] are connected using the cipher text and access policies with the aid of private keys. In KP-ABE, regarding the access to the encrypted data can be done only by the data owners.

CP-ABE [119] is the enhanced version of KPABE in which the access policies are integrated in the cipher text and with the help of private keys the attributes are linked. The access policies should be satisfied by the private key for accessing a particular cipher text. Classification of the ABE scheme is done on the basis of the entire authorities engaged in controlling the attributes. Classification is done as Single Authority-ABE (SA-ABE) and the Multiple Authorities-ABE (MA-ABE). In SA-ABE a single authority is concerned which

observers the overall attributes and the decryption or encryption reports are assigned to the data owner or the user. Hence, the user recognises the attributes of a user and capably decrypts the data. The privacy of the user may be ruptured in the case of corruption and achieving the data confidentiality becomes complex. MA-ABE overcomes the drawbacks of SA-ABE. In MA-ABE the attributes arte monitored using numerous authorities with the dispersal of the decryption or the encryption reference. Therefore, when compared to SA-ABE it is a secured and a conventional scheme [120]. Access control provides authorization and the encryption techniques assure the secured storage whereas the user requires data integrity for storing the data in the cloud. The cloud user's data integrity is checked using the digital signature technique. The Cloud Security Alliance (CSA) has submitted an analysis report in 2013 and as per it cloud framework is exposed to data breach, downtimes also outages. The CSA released a white paper in that data leakage, hardware crash and vulnerable API's are some of the cloud vulnerabilities. The auditing process or guarantee of data integrity is a desirable security aspect for ensuring the cloud users information. The data integrity process verifies the rightness of the data deposited in the cloud database and the traditional cryptography doesn't have data auditing process. In the cloud the data auditing process has been built mainly on the Public Key Infrastructure (PKI). For the certificate users the PKI own digital certificates, offered by the certificated Authority (CA).

3.2 PROPOSED FRAMEWORK

3.2.1 Preliminaries

3.2.1.1 Bilinear maps

The two multiplicative cyclic groups be G_1 and G_T with the prime order p[121]. The initiator of G_1 be g and the bi-linear map is e, $e: G_1 \times G_1 \rightarrow G_T$, having the subsequent features:

$$Bilinearity: for \text{ all } g, g \in G_1 \text{ and } a, b \in Z_p, e(g^a, g^b) = e(g\ , g\ )^{ab}$$

$$Non-degeneracy: e(g, g) \neq 1$$

3.2.2 CP-ABE framework

Setup: The universal attributes is considered as a parameter by this setup algorithm and uses the key authority for execution which generate a master key and public parameters [122].

KeyGen: The key authority executes this KeyGen algorithm and produces the secret key

Encrypt: A message M is achieved by this encryption algorithm and encrypts it with the help of the public parameters.

Decrypt: The user executes this algorithm using the secret key of the user and the cipher text obtained from the cloud.

3.2.3 AES–Cryptology

The proposed model employs the AES algorithm to accomplish a secret operation with the *Lightweight* CP–ABE by 14 rounds using a 256-bit key. Figure 3.1 below illustrates the mechanism of the AES algorithm for encryption.

Besides the Lightweight CP-ABE key, the AES key generated and shared with the user.

- $E_{nc}(\widehat{M}, K)$: Provided the key (K), the final cipher-text $(\widehat{E}_{ct})$ is yielded by the message $\widehat{M}$ in encoding (E_{nc}).
- $D_{ec}(K, \widehat{E}_{ct})$: Provided the key (K), during decoding (D_{ec}) this approach produces the message $\widehat{M}$ from $\widehat{E}_{ct}$.

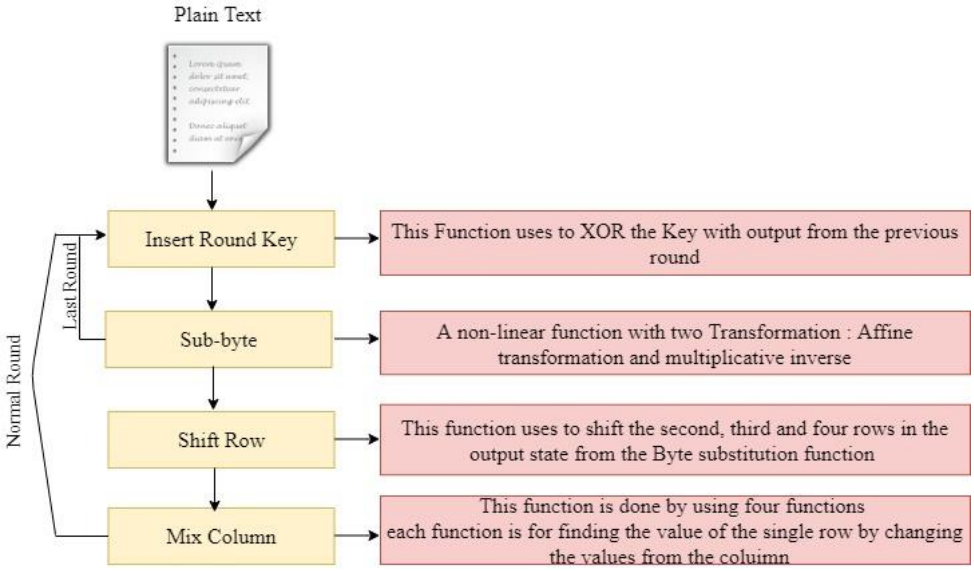


Figure 3.1. Advanced encryption standard

3.2.4 Digital Signature

- $Sign_{Gen}(ID_U, A_T, M_K)$: The digital signature (S_D) is generated by the access policy (A_T), user identity (ID_U) with the master key (M_K) and the message (M_V).

3.2.5 Functioning of the Proposed Scheme

The proposed scheme is depicted in Figure 3.2 which comprises of three crucial modules, as described below:

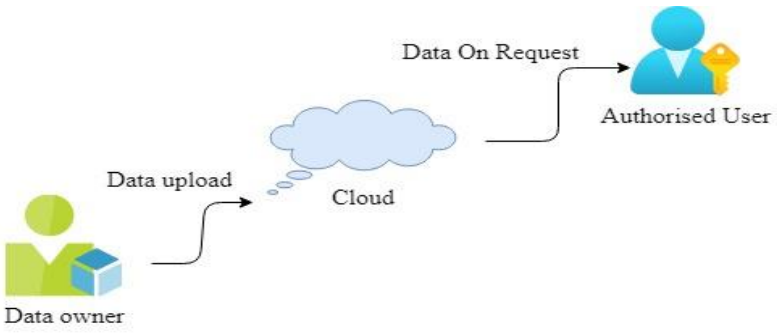


Figure 3.2. Modules of the proposed system

- Data owner: The data owner performs a vital role in the cloud framework. Any authorized user can access the data stored in cloud. The data is uploaded with the help of them into the definite cloud and using the proposed AES–*Lightweight* CP–ABE it is encrypted.
- Cloud server: It is the core of the proposed scheme which secures the cloud framework. The server consists of the stored data from the users and the data owners. It contains the digital signature and the keys of the users, besides their attributes and ID. The reason for designing the servers is to validate the variations amongst the owner's and the user's access to the cloud framework. In the cloud, along with the user authentication, utilization of resource is also monitored.
- Data user: The data that is stored on the cloud is utilised by the data users. Moreover using the authentication keys it decrypts the encrypted data. Based on the permission attributes and identity, the cloud server has to authorize the data stored in cloud.

3.2.6 Security Model and Control Mechanism

In the cloud environment sufficient security to the data could be provided by the proposed framework by adopting three types of control mechanism, as depicted in Figure 3.3. Data security is guaranteed by the proposed framework. The three types of control systems are explicated subsequently:

- Control I: To access the cloud, the CSP and the data owner offers separate authentication. The access policy in the cloud is assigned by the data owner. Therefore, the user accessed the data only by decrypting it.
- Control II: User validation is done by the cloud server.

- Control III: In this model the user is monitor by the data owner for conserving the resource usage.

In the proposed scheme, the security of the cloud environment is described below:

- Access control: For user authentication, the user ID's and their attributes are used so that easily the initial login process cannot be breached by the attacker. Along with this, while the information of the user is being processed for authenticating certain questions randomly will pop up which are linked to the attributes. Only after the verification of the answers the user will be allowed to enter the cloud environment. In the proposed model, a separate authentication process is provided for the data owner and the cloud service providers.
- Data privacy: AES is secure against any instinctual force attacks and has never been broken yet, moreover it is contrary to general beliefs and opinions.

Moreover, because of its symmetry of AES key even if the attacker somehow breaches it, they will come to know the novel *Lightweight* CP–ABE key makes it complex to obtain the actual data. The data privacy is secured using the double encryption process and with AES and *Lightweight* CP-ABE the decryption is carried out.

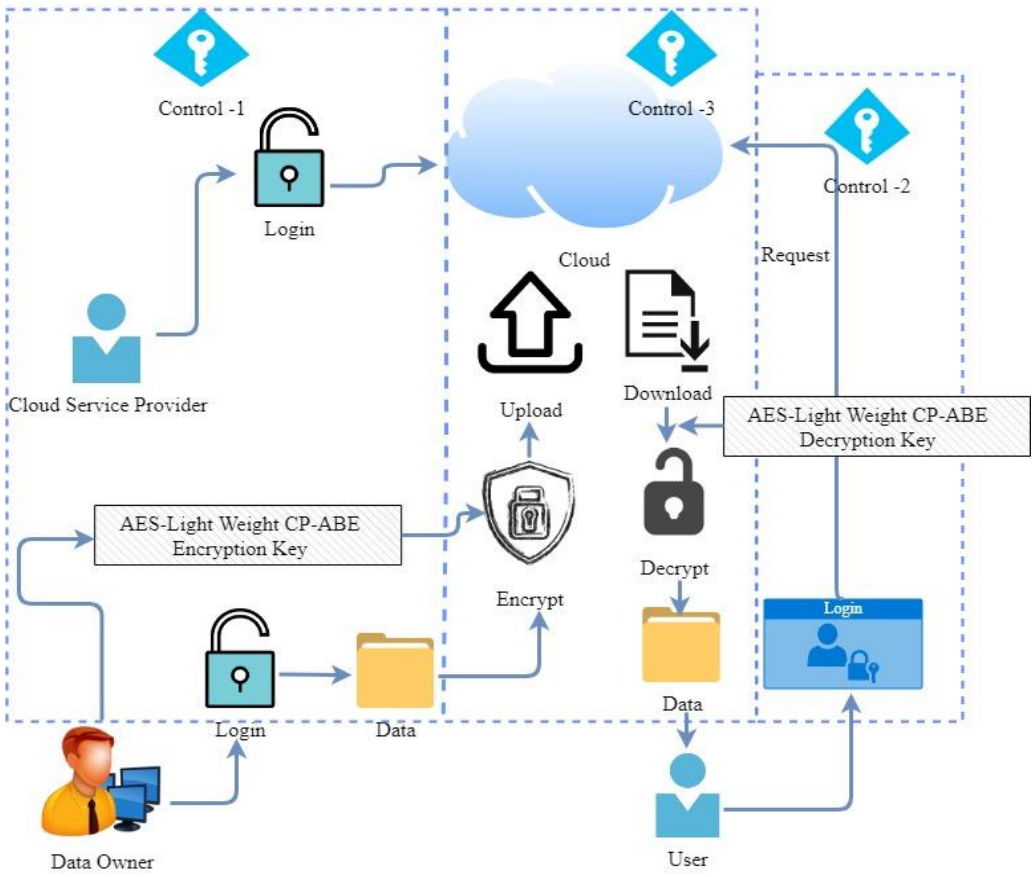


Figure 3.3.Framework designed for securing data privacy

3.2.7 The Flow of Control for the Proposed Algorithm

Three different phases are presented in the proposed framework which involves the digital signature and the *Lightweight* cryptographic keys generation in the cloud server (CS). The input and output variables used in this algorithm are defined below:

3.2.7.1Construction of Lightweight CP-ABE

The proposed *Lightweigh*t CP-ABE scheme is designed based on defined algorithms

SetUp($N \dashrightarrow P_K, M_{SK}$)

Here, T_A produces P_K and M_{SK} as below:

- Along with the bilinear map $e: G_1 \times G_2 \rightarrow G_T$,choose a generator g of group G_1.
- Select randomly $y, t_1, t_2, ...t_n \in Z_P$
- Evaluate $Y = e(g,g)^y, T_i = g^{ti} (i \in N) for\ every$ attribute $i \in N$

KeyGen (M_K, A ⇢ U_{SK})

This algorithm performs the subsequent steps to form the U_{SK} from the attribute set $A = \{a_1, ...a_n\}$

- A random number $r \in Z_p$ is generated.
- from the following formula generate the bit string (B):

  $for\ i \in I$

  $if\ i \in A \wedge i = i$ then $b_i = 1$

  $else\ b_i = 0$ then, Bit string $B = (b_1, b_2, ...b_n)$

AES- Algorithm

- $\hat{E}_{CT} \leftarrow \hat{M}, K$: For the AES cryptography the input given is the decrypted data, again with key (K) and the message $\hat{M}$ the data will be encrypted to $\hat{E}_{CT}$.
- $\hat{M} \leftarrow k, Ect'$: The data will be decrypted with the key (k), and the encrypted data E_{ct} to produce the message $\hat{M}$.

Generation of Signature

- $SD \leftarrow ID_U, A_i M_V$: The CS picks the attributes for producing the digital signature (SD) and user identification (ID_U) with the message.

- $Verify \leftarrow S_D$: The user along with the verification message Mv verifies the digital signature SD.

3.3 Results and Analysis

In this section, data set description and experimental set up are given. We have implemented our proposed security framework using a cloud platform called as CloudSim and a number of tests were performed with 4GB of RAM on a 2 GHz machine. The client-side is formed using a Java-supporting Internet browser. Using three-parameters the proposed approach was evaluated, i.e.:

- User Execution time: The user response time in the cloud and the determined time taken for generating the key.
- Communication of the cloud user: The total volume of data that is expended throughout the communication of the cloud server and the user.
- Upload communication of the data owner: The total volume of data expended to upload the data from the data owners' side.

The subsequent subsections presents the comparison of the proposed made with the existing system.

3.3.1 Execution and Communication Time of the Cloud User

The proposed method's communication assessment was found to be nearly 1000 KB. The basic ABE also achieved the similar value. Resulting that the transmission of data in cloud is not affected by the improvement in the basic ABE, as revealed in Figure 4. The time of execution when compared with the existing, the proposed model was lower than the existing models. Than the ABE method the proposed model was 7.4% more competent. The execution

time of the data was lowered considerably by utilising the proposed approach, as presented in Figure 3.4.

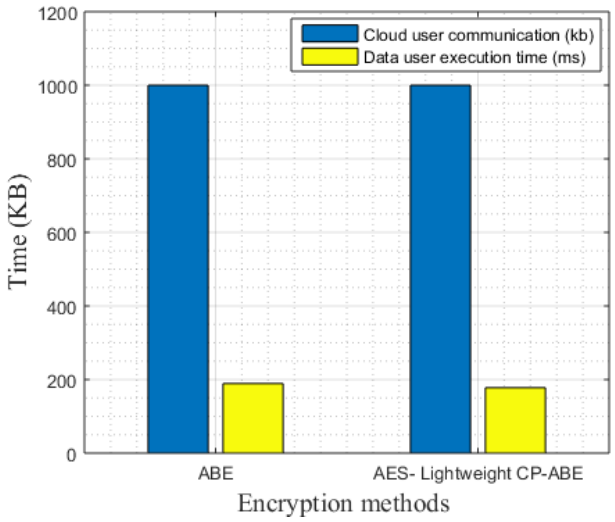


Figure 3.4. Data execution time and User communication graph.

3.3.2 Communication of Data Owner

In the cloud system the data is uploaded by the data owner that can be used by many legitimate users. For uploading the communication an evaluation was conducted for the proposed method with different numbers of users. After validation it was found that the communication of the data owner upsurges with a surge in the number of users. When compared with the existing ABE approach the proposed method attained improved performance with a value of 895 KB whereas ABE attained 989 KB, as presented in Figure 3.5.

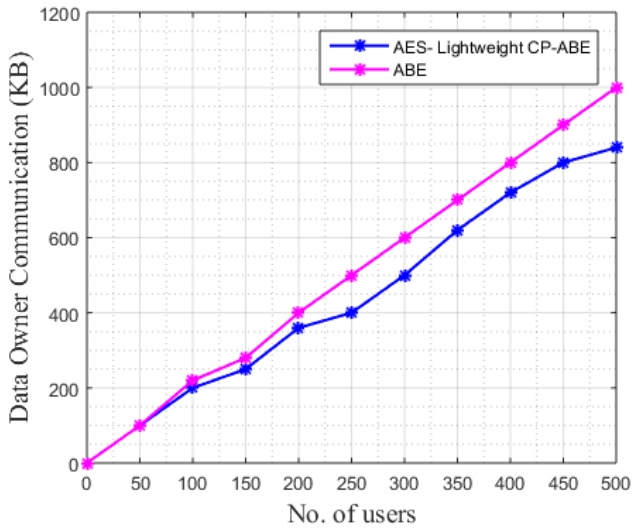


Figure 3.5. The data owner's upload communication graph

3.3.3 Encryption and Decryption Time Cost

Tables 3.1 and 3.2 presents the Encrypting and decrypting time and costs with distinctive-sized data and an aggregate number of cipher-text attributes. The proposed approach attained a rise in the encryption and decryption time when compared with the Improved-CP-ABE (I-CP-ABE) [32] with less number of attributes. The time gets minimised when there is an increase in the attributes. With the attributes of more than 40 KB, the proposed scheme executes in better way. Figures 6 and 7 illustrate the comparison graph for the dissimilar data sizes.

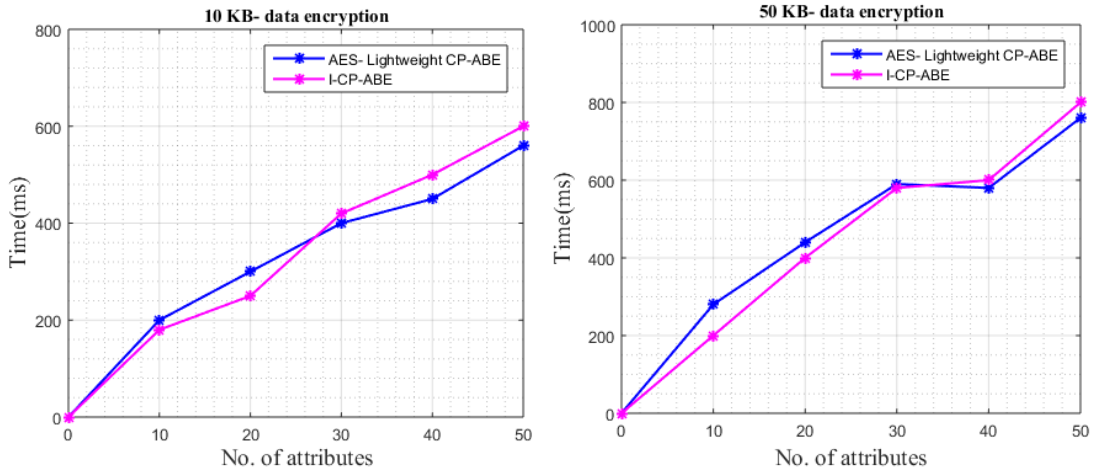
Table 3.1. Encryption time of the proposed and existing methods concerning different data sizes

Size of data	No of attributed	10	20	30	40	50
10kb	I-CP-ABE	100	200	450	550	650
	Proposed	215	277	395	475	555

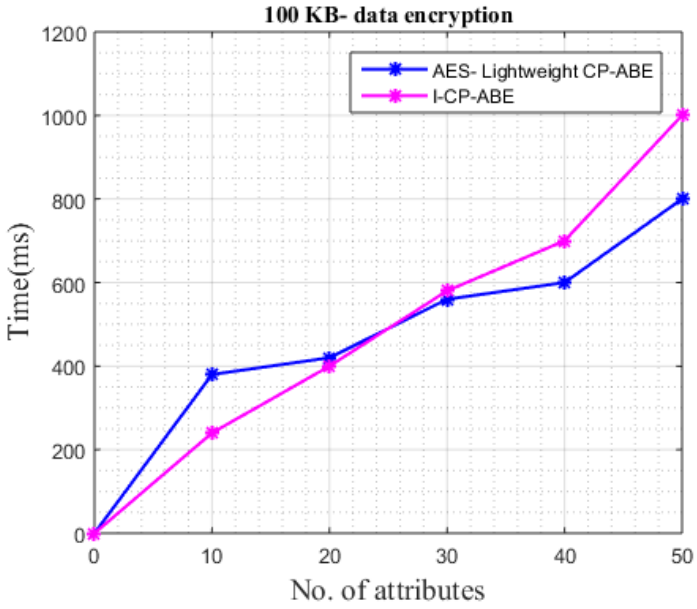
50 Kb	I-CP-ABE	190	400	500	650	750
	Proposed	287	435	560	585	695
100Kb	I-CP-ABE	275	445	650	750	1000
	Proposed	365	485	598	645	855

Table 3.2.Decryption time of the proposed and existing methods concerning different data sizes

Size of Data	No of attributed	10	20	30	40	50
10Kb	I-CP-ABE	80	95	115	155	195
	Proposed	115	120	130	155	175
50Kb	I-CP-ABE	115	135	155	250	350
	Proposed	135	145	155	185	250
100Kb	I-CP-ABE	300	400	450	550	750
	Proposed	300	385	420	530	620

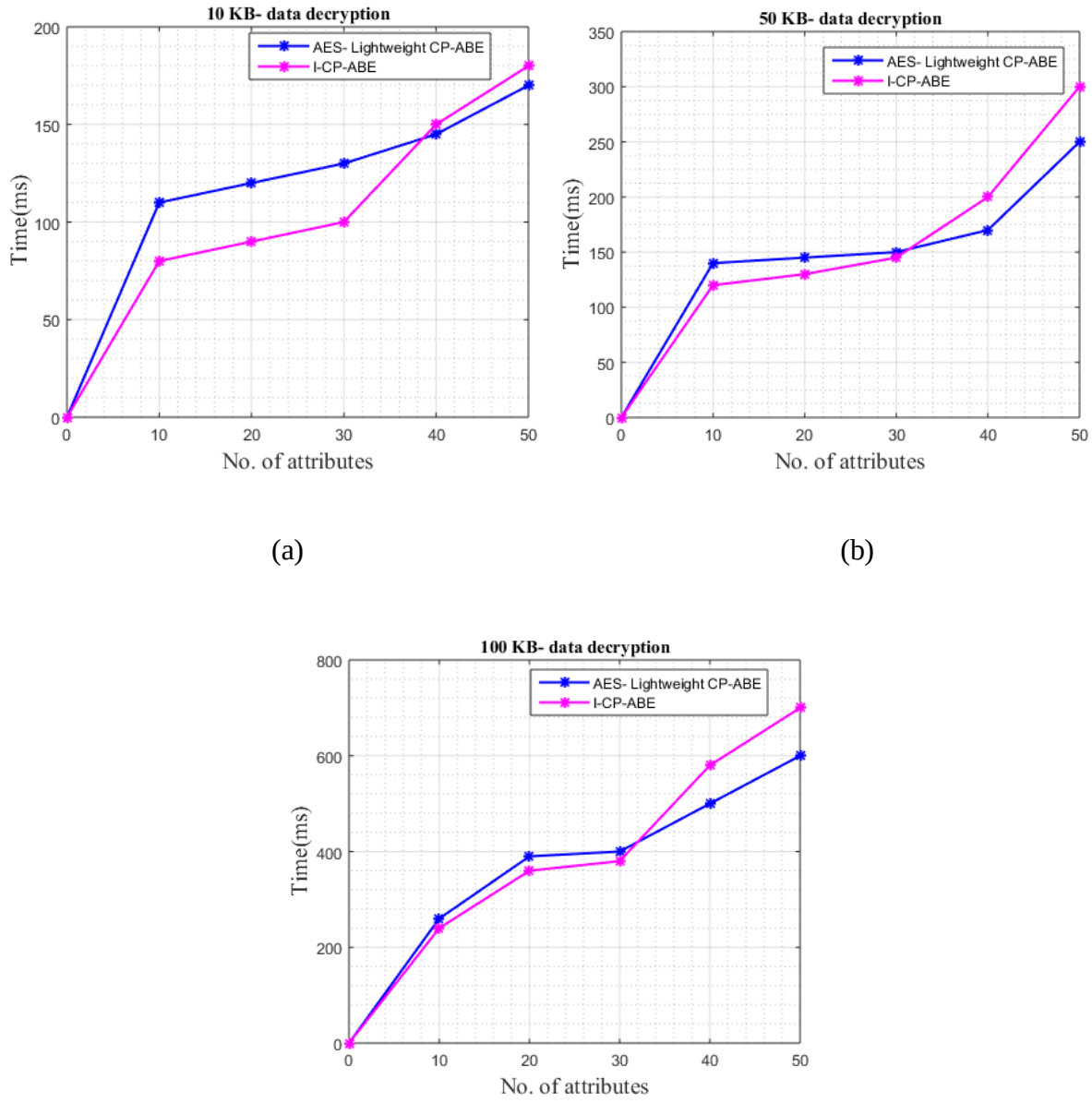


(a) (b)



(c)

Figure 3.6. (a) The encryption graph of the proposed and existing methods with 10 KB data (b) The encryption graph of the proposed and existing methods with 50 KB data (c) The encryption graph of the proposed and existing methods with 100 KB data



(a) (b)

(c)

Figure 3.7. (a) The decryption graph of the proposed and existing methods with 10 KB data (b) The decryption graph of the proposed and existing methods with 50 KB data. (c) The decryption graph of the proposed and existing methods with 100 KB data

3.4 SUMMARY

In the cloud storage space to guard the data privacy the new encryption scheme named, AES *Lightweight* CP–ABE was proposed. Double encryption was performed by the proposed scheme on the cloud data. Initial encryption was done by the *Lightweight* CP-ABE, and using AES the secondary encryption was accomplished. Based on the digital signature the access control was given. The user and the owner acquires authentication in the cloud framework. When the user tries to access cloud, with certain question the attribute set was made that appear randomly. The simulation outcomes revealed that the proposed scheme achieved improved performance than the existing approach with minimum execution time and communication of the data user. As a future enhancement a multi-user cloud environment could be focussed to offer robustness and improved security features. Moreover the proposed approach can be boosted to deal with the user groups and multi-owner character in the cloud more professionally.

CHAPTER IV

SECURE AND RELIABLE DATA SHARING SCHEME USING AES WITH WEIGHTED ATTRIBUTE-BASED ENCRYPTION IN CLOUD ENVIRONMENT

In this chapter, we proposed a secured data access control using the Advanced Encryption Standard (AES) combined with a weighted attribute-based Encryption (AES-WABE).To encrypt the data, the access control policies are used and weight is assigned according to its significance of each attribute. The outsourced data is stored by the cloud service provider and the attribute authority based on the weight that updates the attributes. To minimise the computational overload the data file is accessed by the receiver corresponding to its weight. The proposed procedure provides resistance for collusion, multiple user security with control of fine-grained access based on protection, reliability and efficiency. On concerning the data collaboration and confidentiality, the performance rating is done related with the Cipher-text Policy–Attribute-based Encryption (CP-ABE) and the hybrid attribute-based encryption (HABE) scheme , access control flexibility, limited decryption, full delegation , verification and partial signing .

4.1 INTRODUCTION

Enormous amount of data can be handled by the storage of cloud which is considered as a magnificent service having effective techniques. Personal and business data's can be stored using this facility, due to this factor lot of enterprises, establishments and individual users also uses it.

The data is uploaded in the cloud by the cloud data provider which is later used by the user, with the help of server of the cloud. The multi-regional, multi-domain and extensive data sharing can be recognised by the cloud storage. The benefits of cloud storage are required

resources, on needed storage, economical, maintenance is effortless and managing the storage of the user's [123, 124]. Even though, there are lot of advantages in the cloud storage service, the main issue in it is the security. Different geographically distributed data centres has access to the stored information in the cloud hence, in database of the cloud the data of the user will not be under the user's control. The cloud user faces privacy and data confidentiality problems while using cloud computing [125].Due to the complications on using this [126,127], the cloud-based data resources can be accessed only by the authorized users. To deal with this the data before uploading to the cloud infrastructure should be encrypted, but this approach bounds the sharing and further processing of data [128]. Normally, the encrypted data from the cloud storage is downloaded by the data owner in order to re-encrypt them to share the data. Moreover, the cloud users at some cases act themselves as the content providers. The data is broadcasted by them on the cloud servers so as to share and to access those contents the fine-grained data access control is used. [129-132]. In addition, the contents of data should be confidentially retained by the CSP should against the users of the cloud [133].

Encryption is a spontaneous way to safeguard the data [134, 135]. The essential utilizations of data are blocked by the old-style encryption techniques. To obtain the required data a data user decrypts and downloads all cipher texts from the cloud server. Apparently, this approach will led to computation overhead and unfeasible communication in the cloud computing environment. An inspiration was gained from the author VipulGoyal et al. [136] who proposed a full-blown key-policy attribute-based encryption scheme (KP-ABE). A wide range of access structures is allowed by this method and achieves a flexible and fine-grained data access control using the attribute-based encryption scheme. In this paper, every data's user key is associated with a specific tree-access configuration assisting the threshold gates.

Using the user key the message can be from the final cipher text if attributes of cipher text satisfies key's access structure. The Rivest–Shamir–Adleman (RSA) algorithm connected with the digital signature has been examined to the cloud data for purpose of security which approves the digital message. The attribute based signature (ABS) and group signature is joined to guarantee the consumer anonymity since the attribute authorities are safeguarded by the private key.

In order to remove the constraints and to protect sensitive data the cloud protects the personal data in the cloud silently. Using the fine grained-access control the data encrypted by the owner of data will be deployed to the cloud. At the time of collision the leakage of information might occur between the user and the cloud, and by using the safety data sheet (SDS) leakage of data can be stopped. And the data is protected from vulnerability by employing the similarity index and to support the query of the neighbour's and the m-index is encrypted. The private key of the signer's is divided into dual types using policy attribute based signature (KP-ABS) based on the key. Other users cannot access the signature.

4.2 Attribute-Based on hierarchical Encryption

By combining the features of the hierarchical identity-based encryption (HIBE) and the cipher text-policy-attribute-based encryption (CP-ABE) hierarchical attribute-based encryption (HABE) can be developed. This approach has scalability and supports fine-grained access control moreover yields the entrustment among the attribute authorities. This approach signifies the hierarchical structure of the establishment when compared with other conventional methods, moreover this scheme suits for an outsourcing organization.

CP-ABE: This approach is a reversed form of the KP-ABE scheme which makes the user to clarify the access strategy upon the entire attributes with the intention of the data consumer to

decrypt the cipher text. As a result, the data access control and confidentiality can be assured. The steps involved in this process is stated below

(1) Encrypt (P_K, S_a, m): This stage outputs a cipher text C_T by fetching the inputs P_K, the descriptive attribute Sa and a message m.

(2) Decrypt (C_T, S_K): In this stage the input is C_T , which contains the $(S)_K$ user's secret key and the access tree (T) merged with S_a, message m is the output. When S_a satisfies T this stage is fulfilled.

(3) Setup (): Only unstated security parameter is approved in this stage. The public key P_K and the Master key M_K are created at this step.

(4) Keygen (M_K, AS): In this step the inputs considered are the non-monotonic access structure AS and M_K and provides the output as the attribute secret key S_K. The cipher text is combined with CP-ABE's access image until the pack of detailed attributes makes an interpretation for decryption process as shown above. The decryption key and the cipher text is changed with the influence of KP-ABE. Moreover, this system, along with a threshold value provides the monotonic access form for appropriate attributes. The CP-ABE approach is effectual in respect of enforcing the access control of the encrypted data than the approach of KP-ABE. The bound of CP-ABE is that it fails to fulfil the efficiency and flexible properties of the provisions in their access control.

HIBE: This approach is the prolongation of IBE .The primitive ID (PID) of public keys is used by a private key generator (PKG) that delivers the private key and referred as 1-HIBE. This approach has heavy key handling which is an imitation of this scheme. A 2-HIBE approach is used to deal with this; it has a root PKG and a domain PKG. The domain PKG generates the domain secret and creates the secret key which is achieved from the root of

private key generator. The cryptosystem comprises of authority of a root certificate that allows the certificates of hierarchy .Besides, HABE degrades the support for multivalued tasks and cannot capably aid the compound attributes. A novel AES-WABE method is presented in this study to deal with this drawback.

4.3 PROPOSED FRAMEWORK

By the proposed AES-WABE approach a protective and efficient data association is reached. A unique access is used to deal both the secret and public keys by the existing ABE methods. In specific situation the attributes the consumers manages the attributes from multiple authorization of the attributes and the data holders shares the data of the consumers and it is controlled by the different authority. To deal with this problem several attribute-based multi authority access control structures are proposed. To provide secure data, in this study the weighing of attributes is given by the AES. Five basic modules are considered in this system: (a) a cloud server for storing the data (b); the data holder, who uses an access control policy for data encoding and uploads it to the cloud; (c) A weight attribute authority (WAA) based authorization, this validates and updates the users attributes; (d) the Central Authority (CA), grants a global user identifier and consumer public key for every consumers to WAA; and (e) the data users, as shown in Figure 4.1. The weighted attributed authority is combined with the AES which is presented in the Figure 4.1.

The AES used in the proposed approach generates the keys randomly by encrypting and decrypting the data. Moreover for security purposes an image-matching technique is employed. Later, a weight value is generated by the system for the users based on its attributes.

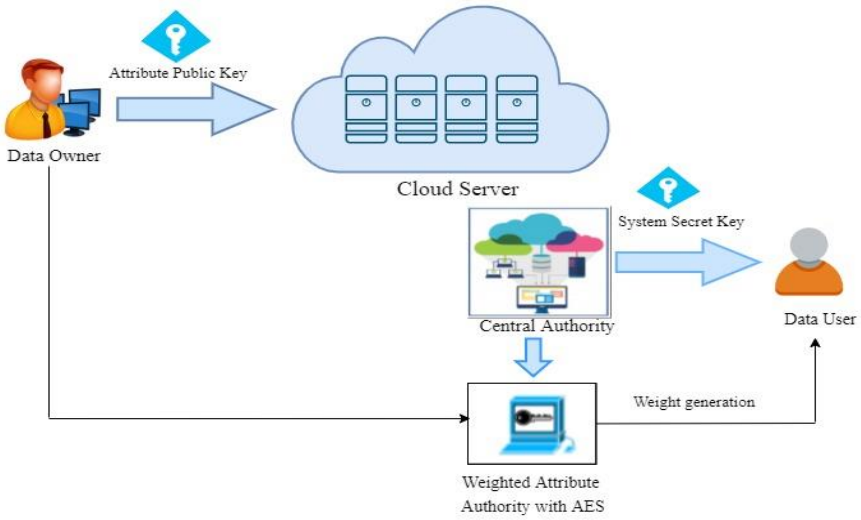


Figure 4.1. The Proposed Framework (AES-WABE)

This scheme is reliable and secure; while comparing with the conventional methods this approach is suitable for applications in real-time. Proposed encryption considers multi authority security, collusion resistance along with fine-grained access control. Two phases are available in the proposed method and that includes the system phase, algorithm phase. In the phase of algorithm, the system-level operations are defined with the AES algorithm. In conflict, the foremost operations for example, User Annulment, System Setup, admitting New User, Creation of New File, File Access and Deletion are described in the system level.

4.3.1. Operations in Algorithm Level

4.3.1.1 AES Encryption

AES [137] is the alliance of permutation and substitution which is according to the substitution-permutation network and it has high efficiency in the hardware and software. This system does not use a Feistel network **u**nlike its predecessor DES, AES. AES is a form of Rijndael which has a key size of 128, 192, or 256 bits and a fixed block size of 128 bits, and illustrated in Figure 4.2.

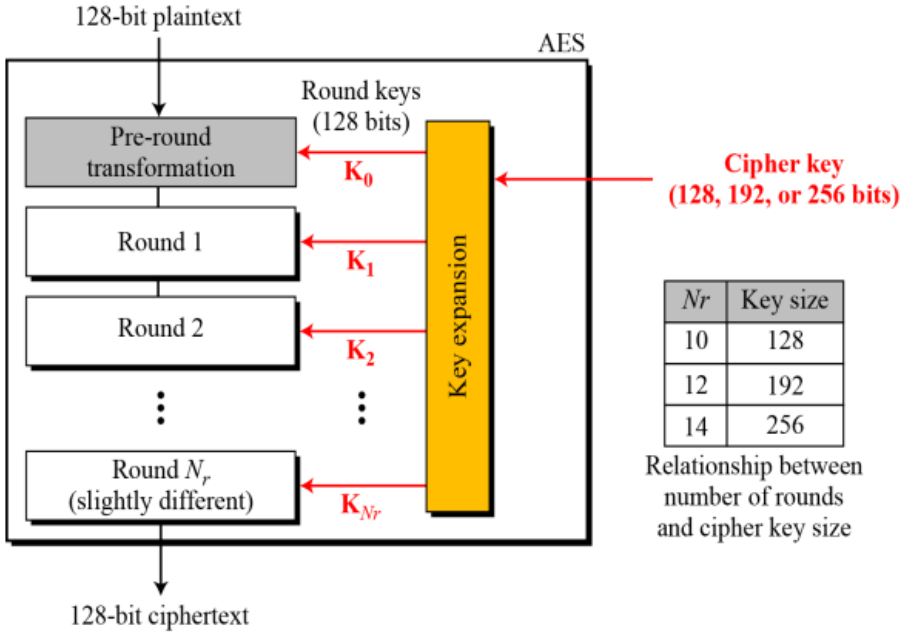


Fig. 4.2. AES Encryption process

For an AES cipher the key size used states the number of replications of transformation rounds that convert the input, i.e. the plaintext, into the final output, i.e. the cipher text. The following are the number of cycles of repetition:

- 14 cycles for 256-bit keys repetition
- 12 cycles for 192-bit keys repetition.
- . 10 cycles for 128-bit keys repetition

There are certain processing steps for each round; each has four similar but dissimilar stages.

To transform the cipher text into a plaintext pair of reverse rounds is implemented using the similar key of encryption. Four types of transformations are used by AES to provide security they are mentioned below.

- Permutation: This stage does is a transposition in which each row of the state is shifted to a certain number of steps.

- Substitution: In this particular stage based on the lookup table each byte is replaced with another.
- Mixing: This stage functions on the state columns; in each column four bytes are combined.
- Key-Adding: At this stage, the state unites the partial key an in every round a sub key is obtained from the main key by using the schedule of Rijndael's key; the sub key size is similar to that of the state. On combining the bytes of the state with the sub key it uses the bitwise XOR operator. The AES Encryption/ Decryption algorithm is mentioned below.

Algorithm for Encryption of AES

```
Cipher ((byte out [4*Nb]), (word
W [Nb*(Nr+1)]), (byte in [4*Nb]))
Start
    Byte condition ([ Nb,4])
    condition = in
    AddingRoundKey ((w [0, Nb-1]), condition)
    For round = 1 from step 1 to Nr–1
        (condition) Shift Rows
        (condition) Sub Bytes
        (condition)Mix Columns
        (condition)Adding RoundKey ,
        W (([(round+1)*Nb-1]), (round*Nb))
    End for
    (condition)Shift Rows
```

(condition)Sub Bytes

AddingRoundKey ((w, condition [Nr*Nb),

(Nr+1)*Nb-1]))

condition = Out

Quit

Algorithm for Decryption of AES

InverseCipher ((byte out [4*Nb]), (word

W [Nb*(Nr+1)]),(byte in [4*Nb]))

Start

Byte condition [Nb,4]

In= condition

AddingRoundKey ((w [Nr*Nb),

(Nr+1)*Nb-1]))

For round = Nr-1 step -1 down to 1

(condition) InverseShiftRows

(condition)Adding RoundKey ((W [round* Nb), (condition), ((round+1)*Nb-1]))

(condition)InverseMixColumns

End for

InverseShiftRows (condition)

InverseSubBytes (condition)

AddingRoundKey ((condition), (w [0, Nb-1]))

Out = condition

Quit

4.3.2 Process in System Level

This process is defined below:

(1) System Setup: The algorithm for global setup is processed by the challenger to attain the global public parameters. A security parameter is chosen by the data holder which yields the secret key SK by giving a request message to the interface of the phase setup of the algorithm.

The Central authority (CA) receives every SK component that is cyphered by the data holder and encrypted module once it is sent.

Despite, the holder's signature is authenticated by the CA. Moreover, if it's correct the CA uses the systems public and master key which provides a secret and public keys for a new consumer. The attributes weight is determined by the WAA in the organization domain.

(2) Key Generation: CA allots an uncommon user ID while the system is connected with the new user.

Conversely, the consumer of the attribute set is cyphered and sends it to the WAA. The consumer's signature is authenticated by the attribute authority.

If it is true, WAA creates the weight for the new consumer and the equivalent attribute secret keys. Next, the WAA and CA, separately, transfer the attribute secret key and the consumer's system secret key to the new consumer.

Ongoing with the setup of the central authority and the relating keys algorithm the challenger prevails and issues the hackers public keys.

(3) Encryption: Prior posting the data file by the data holder, for encoding the data an uncommon ID is used to log in and employing for symmetric data file key of encryption. For

respective data files and users, the "weighted threshold access structure" (W) is defined by the data holder and the usage of W data is encrypted as shown in Figure 4.3.

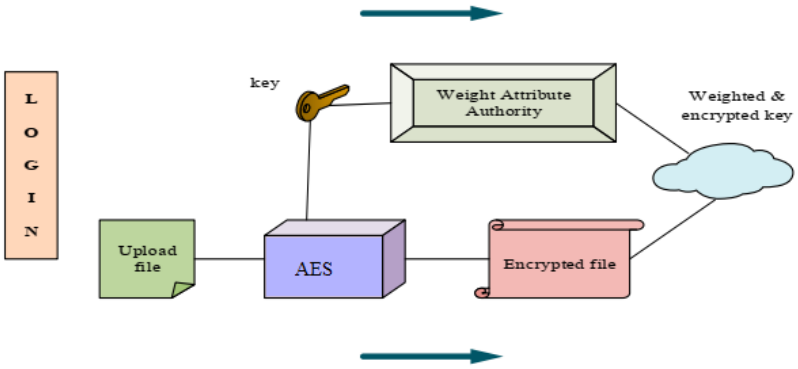


Figure 4.3. Process of encryption on the owner side data

(4) Decryption: The data is downloaded by the consumer from the cloud, and then decrypted the information using the decryption algorithm. Suppose the attributed secret key of the data consumer is approved, then the system grants different weights as per their level.

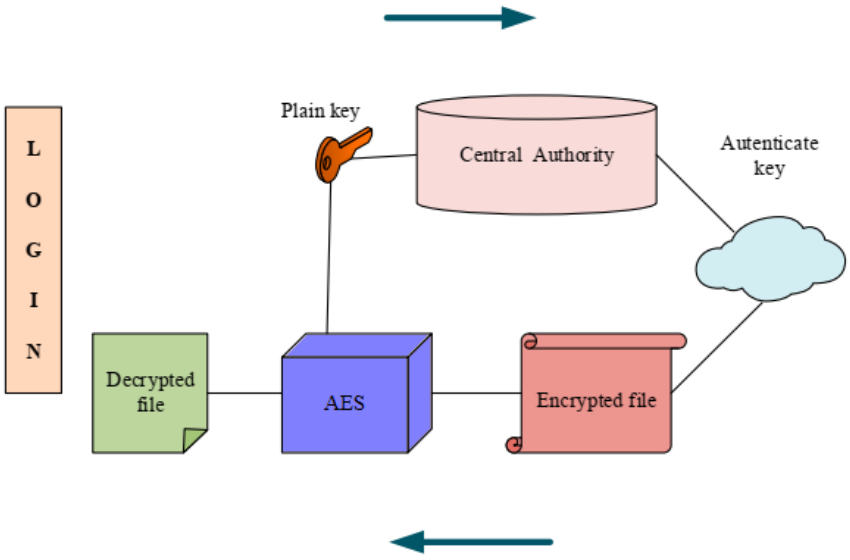


Figure 4.4. Decryption process of the data user side

Then, with respect to W the user decrypts the respective data file. If the user is invalidated the user fails for data file decryption, as shown in Figure 4.4.

4.4 Results and Analysis of the Experiment

In this section we have experimented and analysed the performance of the proposed work. This work is done using the language Java with 8GB RAM (Random access memory) and Intel core i3 processor. The cost of computation is calculated for encryption and decryption. Even though these systems achieve the access control of encrypted data in the cloud network it provides security of data. The existing methods CP-ABE [34] and HABE [35] are compared with the data collaboration schemes of the proposed approach. The proposed approach attains full delegation and partial signing with less workload (WAA and data user) and in a large-scale consumer this achieves the lightweight key management. The AES approach employed in this study encrypts and decrypts many input files of dissimilar sizes (in kB) and also does weight generation and Key generation. Mainly for security function this AES algorithm. This algorithms does the encryption and decryption process with very less execution time. Table 4.1 illustrates the final results of the approach of proposed system.

Table 4.1. Experimental outcomes of throughput, encryption/decryption and execution time for AES-WABE

Input data	Size of the File(GB)	Encryption Time	Decryption Time	Throughput
I_1	1	120	115	0.00850
I_2	2	235	226	0.00870
I_3	3	344	600	0.00876

Time of Encryption: The time of Encryption is stated as the required time for data encryption. It is used to validate the system speed and to assess the throughput of an encryption approach. The encryption time is the time required to create ciphertext from plaintext. Figure 4.5 illustrates the encryption time.

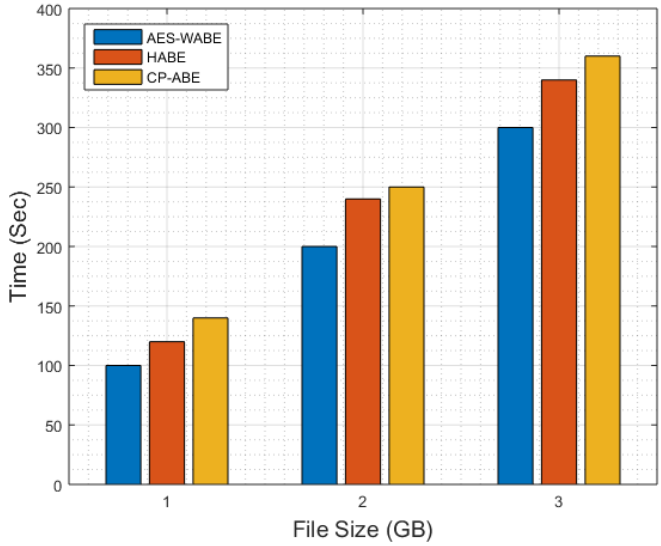


Figure 4.5. The Encryption time of the proposed compared with the existing

Decryption time: The decryption is the converse process of encryption process. The time taken to yield a plaintext from a cipher text is termed as the decryption time. Figure 4.6 illustrates the decryption time of the proposed compared with the conventional methods.

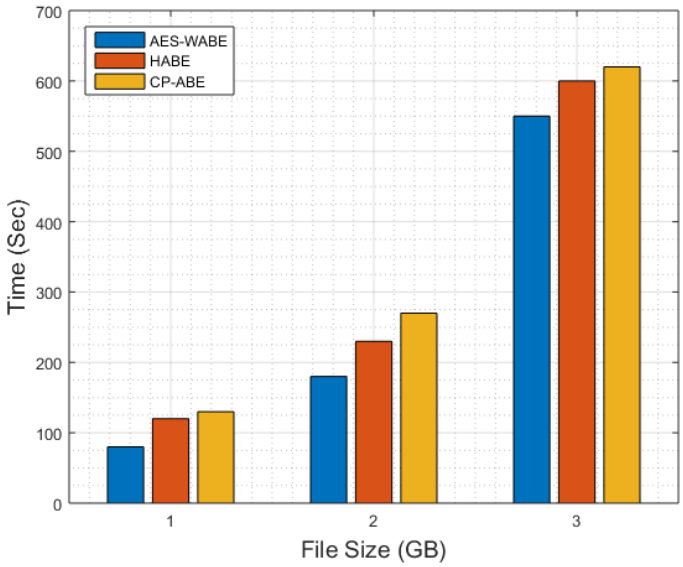


Figure 4.6. The decryption time of the proposed method compared with the existing methods

Throughput: Throughput is defined as the ratio of the file of data which is encrypted based on the encryption time. The proposed approach achieves high throughput as per the figure 4.7.

$$Throughput = \frac{\text{Size of the file (Kb)}}{\text{Encryption Time}} \quad (1)$$

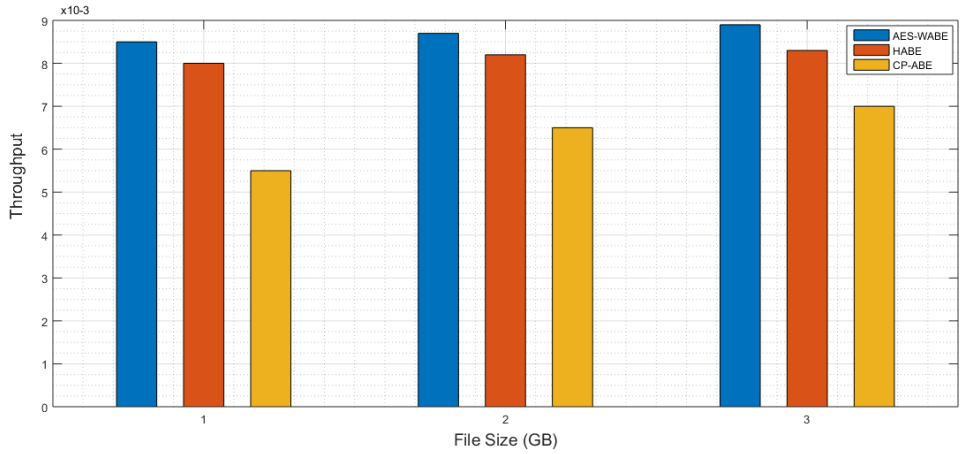
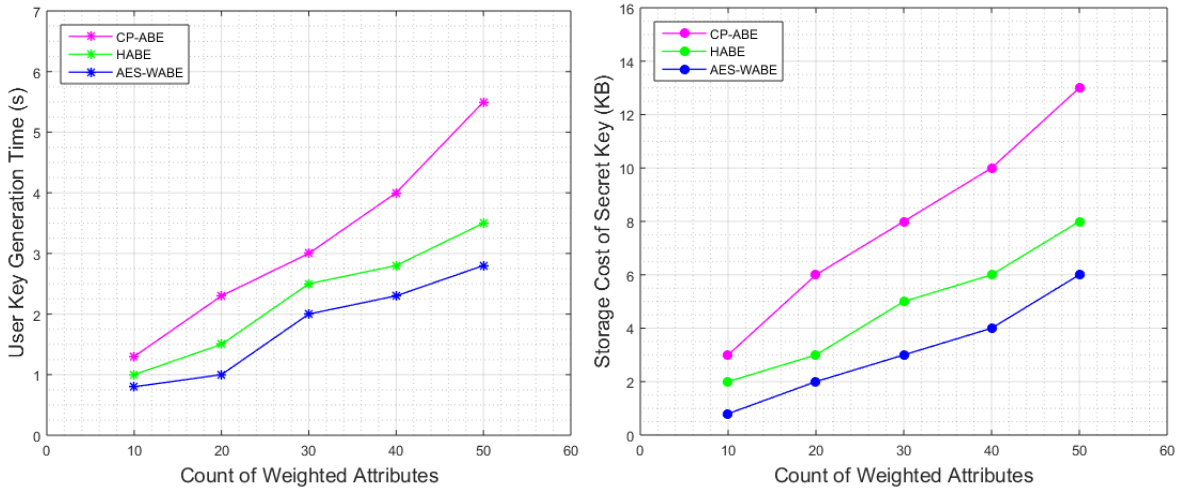


Figure 4.7. Throughput Comparison of CPABE, HABE and AES-WABE

Secret key analysis Rate: In Figure 4.8, an analysis of the overhead storage and the cost of computation of secret key is done and plotted. The total number of weighted attributes and the storage overhead or time cost is represented in the X and Y axis.



(1) (2)

Figure 4.8: Cost generation of User secret key: 1, and cost analysis of time 2 storage analysis.

Cipher text analysis cost: Figure 4.9 illustrates the cost of computation and storage elevation of data encryption. X and Y axis denotes the number of weighted attributes and the time cost or storage overhead of data encryption.

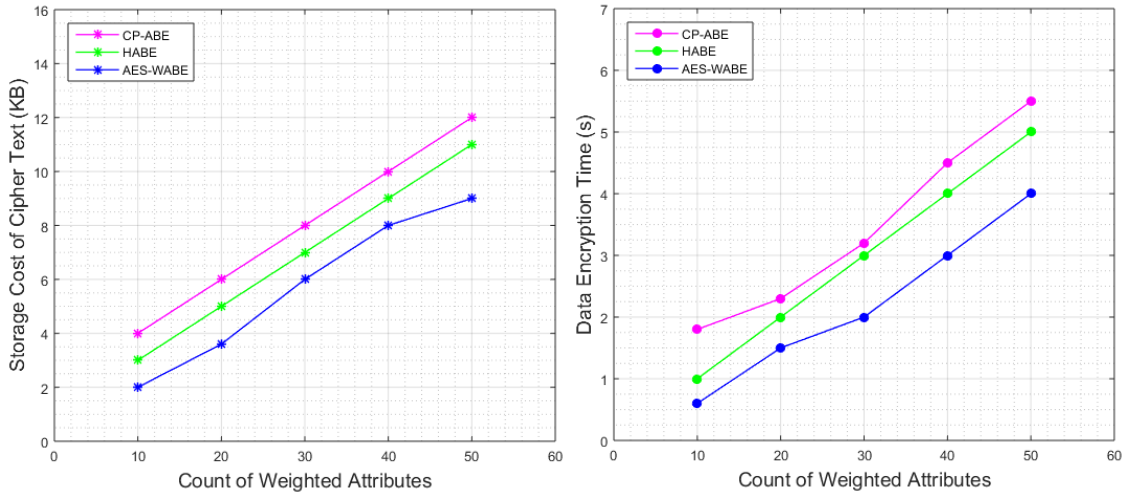


Figure 4.9. Cipher text cost. (a) Analysis of Storage cost; (b) Analysis of Time cost

4.4.1 Security Analysis

The proposed AES-WABE technique encrypts shared data. The protective features of the proposed scheme is analysed as follows:

4.4.2 Fine-Grained Access control:

This scheme provides flexible differential access policies for individual data. The AES-WABE scheme is used to implement this kind of access control. In the encryption phase of the proposed scheme, a flexible and expressive access policy is enforced by the data owner and to encrypt the data the symmetric key is used. The defined access policy in tree undergoes with the access critical operations, ie AND and OR gate, which represents any preferred access conditions.

4.4.3 Data confidentiality:

Access policy is used for encryption, which guarantees data confidentiality against the users which fulfil the access policy without maintaining the attributes set. In a cipher text, the access policy cannot be satisfied by the set of attributes during the decryption phase, the value A = e (h, h)gt cannot be recovered to attain the anticipated value of the global key (G_K). Thus ,the user decrypts cipher text with reasonable attributes that satisfy the policy of accessing. CK is a random symmetric key which encrypts the data, it is secured by AES-WABE. Since the AES-WABE and the symmetric encryption scheme are secure, the outsourced data's confidentiality is assured against illicit users.

4.5SUMMARY

User authentication and Data security in the environment of the cloud are the challenging issues. In this study an access control scheme is proposed which is very efficient and

scalable. This study employs an AES Hybridised weight attribute-based encryption mechanism which provides data security. To transmit data securely AES does the encryption and decryption process. When a request is made by the authenticated user, the consumer based on its weight receives the corresponding files in an encrypted format. The generated key with the AES algorithm is used to decrypt the data by the data consumer. The experimental outcomes reveals that the proposed approach is proficient based on efficiency and reliability. In future this work can be extended by providing protection-saving property and quality-based encryption and re-encryption. These are the aspects wherein one can employ miscellaneous methods to achieve information-sharing.

CHAPTER V

CONCLUSION AND FUTURE WORKS

In this chapter, the thesis is concluded and the contributions are summarized. In addition, the chapter concludes with a discussion of future research.

SUMMARY

A virtual machine, technologies, middleware, networking and hardware have made tremendous progress, resulting in the emergence of new, computing platforms providing computation services on a global basis and accessible storage as a service via the Internet. The cloud computing phenomenon is widely recognized as leading the way toward delivering IT services and infrastructure as a new, promising platform.

Cloud models were studied for their properties of simple access, scaling up, and scaling down. Following are characteristics of a cloud computing model that should be used by consumer's confidentiality, integrity, identity, availability and privacy of their data. This research paper reviews problems related to cloud security models. Further, this research work focuses on a secure data transfer model that is created without taking the data's location into account. Validating integrity and providing security assurance for the storage of data is essential for privacy protection. In research studies, cryptographic mechanisms were developed to ensure security. As a first step to implement encryption mechanisms, the security level and vulnerabilities of data access are determined.

A cloud computing service transmits information through the internet to a remote server or PC, enabling it to be stored, maintained, and processed. For many cloud service providers, password

authentication entails maintaining a verification table. The stored requirement of the verification information of the User compromises the security of authentication. In addition to using Two-Factor Authentication, service providers also provide two-step authentication methods. There are many one-time password techniques, which are based on securing the server's public key seed using a one-time password system (OTP). Also, there are no solutions that simultaneously satisfy two different categories of authentication requirements. Researchers propose a method for providing a secure and flexible authentication mechanism in their research.

Whether it's an individual user or a resource within an organization or a virtual machine in a cloud environment, everything is connected as the object-oriented technologies represent them as objects. As part of the object-oriented development process, these objects are related. The access control mechanism is developed using these two facts. A means for controlling access by utilizing object relations is built on the reality of object relations. Data storage is moving towards the cloud with the convergence of the internet, in order to meet and control access to the cloud, the access control mechanism is designed.

As the future of the IT industry develops in cloud computing environments, security and privacy protection become more important. In a cloud computing environment, the security of data authentication is crucial to maintaining privacy.

Assigning tasks to the cloud is one of the crucial processes that allow optimal resource allocation among given tasks to provide the desired quality of service. In cloud computing, the scheduling process mostly focuses on tasks, VMs, and PMs.

Considering the high amount of energy necessary for processing such a large number of VMs, energy consumption is the biggest challenge. The main concerns for power consumption in a data center are Memory usage, I/O and CPU. With a power consumption-based cloud resource scheduler, you can enhance resource utilization, while reducing cloud energy consumption. QoS is a major concept involved in task scheduling for obtaining better results on the basis of satisfying user requirements and improving overall performance in the cloud data centers. Virtualization enables a more efficient way to maximize computing power while improving data center QoS.

Its main objective is to provide a solution to the problem of data security that is the main concern of anyone looking to adopt cloud services. An attack protection framework has been created in the cloud environment that will shield data, messages, and information from a variety of attacks. Authentication is done in three stages, data access is secured, and it is publicly verified. In addition to protecting against unauthorized access and untrusted servers, the method is also protected against third-party verification.

As a result of experiments, the proposed method shows to be very efficient, but there is one disadvantage, during data modification, the tags and blocks must be updated, incurring computation and communication costs. With a decentralized double encryption mechanism, scalability, and data confidentiality, it is possible to work in a more secure manner.

In addition to delegating computation-intensive tasks to cloud servers, the proposed system protects the content of the data without disclosing it to the data owner or information about user privileges, as well as accountability. It is observed that sharing medical information on cloud

platforms is feasible, economical, efficient, flexible and more beneficial to human beings. The "Advanced Encryption Standard with *Lightweight* Cipher-text-Identity and Attribute-based Encryption" (AES– Lightweight CP–ABE) mainly to defense data privacy.

Future Works

Considering the cost advantage cloud computing provides for running a business enterprise, its adoption is inevitable, unavoidable, and un-ignorable. A virtual environment provides all employees, system resources, including computing power, at the lowest cost possible. All the e-commerce companies we see like Amazon.com, Flipkart, E-Bay, etc. are not in the process of integrating blockchain technology, this could have occurred due to the high cost of IT infrastructure in the absence of the cloud. Thus, cloud computing research is needed to tackle a wide variety of problems, which is why it is urgent to encourage its further development. Multiple concerns exist regarding the adoption of the cloud, including network security, data security, the integrity of data, access control, and authentication. Research in any of these fields would provide better insights into how organizations could adopt cloud more confidently, easily, and profitably. Our thesis contains the basic research work required for the implementation of the algorithms we propose in network security, data security, and cloud adoption. By doing so, it will reduce the risk of security threats, including network security and data security threats.

By implementing the proposed algorithm with existing tools and techniques, we can solve cloud network problems in an efficient and secure manner. So that changing their business model by migrating to the cloud. It is possible that the industry could use our survey results to improve

cloud security in the future by enhancing adaptation, prevalent awareness, and improving the security of cloud networks.

It is important to create standards that will strengthen the security level of cloud computing in the future. The cloud may offer many benefits for ensuring the safety of data, but none of them is a definitive solution for securing data in the cloud. To resolve this issue, new standards can be established for all the techniques developed in the past and it can be made a requirement that for a technique to cease termination, it must satisfy the devised standards.

The standards can be made mandatory for techniques to cease termination after they have met them. Rather than having standards for interoperability with other providers, there are no standard requirements. A similar drawback leaves the system vulnerable to attack, the interoperability of a system that is used exclusively for data authentication is essential. A cloud will have a high level of data exposure when interacting with another system, The result of this is that data leaks occur, requiring upgraded standard development.

In the near future, most of our work of developing a well-defined and appropriate standard will be focused on the efficient operation of the system. We will also focus on standardization and creating a policy-based access control system for users that will enable them to access information that would enhance the cloud's safety level. Various security concerns would arise from the multilevel sharing of resources. However, the work accomplished so far has alleviated this to an extent, and further updates can be made on this as well.

Our goal is to extend our proposed work for real-time applications incorporated into public clouds along with public auditing services which in addition, it offers public auditing services.

Additionally, we will explore the possibility of implementing the proposed scheme in a federated cloud where we integrate multiple clouds and there are multiple providers of cloud services available to customers. Also, to enhance the access control solution to implement it in real-time applications and to integrate the data auditing feature into the suggested scheme to ensure the data is valid. If we conduct higher-level research in this direction, we can reach solutions that would greatly benefit the organizations in terms of reduced cost of doing business, transparency, virtual availability, mobility, and portability.

PAUBLICATIONS

1. **Chandrajeet Yadav, B.D.K Patro**, **Vikash Yadav, "AES-Light Weight CP-ABE Based Privacy Protection with Effective Access Control Mechanism in Cloud Framework"**, Design Engineering, Rogers Media Publishing Ltd., ISSN 0011-9342, Vol. 2021, No. 6, pp. 2321-2336, June 2021, Indexed in **Scopus**.

2. **Chandrajeet Yadav, B.D.K Patro**, **Vikash Yadav**, **"Authentication, Access Control, VM Allocation and Energy efficiency towards Securing Computing Environment in Cloud Computing"**, Annals of the Romanian Society for Cell Biology, Association of Cell Biology Romania Publication, ISSN 1583-6258, Vol. 25, No. 6, pp. 17939-17954, June 2021.

REFERENCES

[1] Fithri, D.L., Utomo, A.P. and Nugraha, F., 2020. Implementation of SaaS cloud computing services on E-learning applications (case study: PGRI foundation school). In Journal of Physics: Conference Series (Vol. 1430, No. 1, p. 012049). IOP Publishing.

[2] Mrozek, D., 2020. A review of Cloud computing technologies for comprehensive microRNA analyses. Computational Biology and Chemistry, p.107365.

[3] Murthy, C.V.B., Shri, M.L., Kadry, S. and Lim, S., 2020. Blockchain based cloud computing: Architecture and research challenges. IEEE Access, 8, pp.205190-205205.

[4] Loubière, P. and Tomassetti, L., 2020. Towards cloud computing. TORUS 1–Toward an Open Resource Using Services: Cloud Computing for Environmental Data, pp.179-189.

[5] Alshouiliy, K. and Agrawal, D.P., 2021. Confluence of 4g lte, 5g, fog, and cloud computing and understanding security issues. In Fog/Edge Computing For Security, Privacy, and Applications (pp. 3-32). Springer, Cham.

[6] Kumar, A., Krishnamurthi, R., Nayyar, A., Sharma, K., Grover, V. and Hossain, E., 2020. A novel smart healthcare design, simulation, and implementation using healthcare 4.0 processes. IEEE Access, 8, pp.118433-118471.

[7] Jeevitha, J.K. and Athisha, G., 2021. A novel scheduling approach to improve the energy efficiency in cloud computing data centers. Journal of Ambient Intelligence and Humanized Computing, 12(6), pp.6639-6649.

[8] Kaur, J. and Sidhu, B.K., 2017. Task Scheduling in Cloud Computing using Various Techniques. International Journal of Advanced Research in Computer Science, 8(5).

[9] Sadhasivam, N. and Thangaraj, P., 2017. Design of an improved PSO algorithm for workflow scheduling in cloud computing environment. Intelligent Automation & Soft Computing, 23(3), pp.493-500.

[10] Munguti, S. and Opiyo, E., 2018. Factors influencing the adoption of cloud computing in software development companies in Kenya. International Academic Journal of Information Systems and Technology (IAJIST), 2(1), pp.126-144.

[11] Gundu, S.R., Panem, C.A. and Thimmapuram, A., 2020. Real-time cloud-based load balance algorithms and an analysis. SN Computer Science, 1, pp.1-9.

[12] Liu, S., Yue, K., Yang, H., Liu, L., Duan, X. and Guo, T., 2018, May. The Research on SaaS Model Based on Cloud Computing. In 2018 2nd IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC) (pp. 1959-1962). IEEE.

[13] Hadi, F., Aliouat, Z. and Hammoudi, S., 2020. Efficient Platform as a Service (PaaS) Model on Public Cloud for CBIR System. Ingénierie des Systèmes d Inf., 25(2), pp.215-225.

[14] Malla, S. and Christensen, K., 2020. HPC in the cloud: Performance comparison of function as a service (FaaS) vs infrastructure as a service (IaaS). Internet Technology Letters, 3(1), p.e137.

[15] Al-Ahmad, A.S. and Kahtan, H., 2018, July. Cloud Computing Review: Features And Issues. In 2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE) (pp. 1-5). IEEE.

[16] Cohen, A. and Nissim, N., 2018. Trusted detection of ransomware in a private cloud using machine learning methods leveraging meta-features from volatile memory. Expert Systems with Applications, 102, pp.158-178.

[17] Abualigah, L.M. and Diabat, A., 2021. A novel hybrid antlion optimization algorithm for multi-objective task scheduling problems in cloud computing environments. Clust. Comput., 24(1), pp.205-223.

[18] Patel, R.V., Bhoi, D. and Pawar, C.S., 2020. Security Hazards, Attacks and Its Prevention Techniques in Cloud Computing: A Detail Review.

[19] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P. and Sikdar, B., 2019. A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access, 7, pp.82721-82743.

[20] Ahmed, A., Latif, R., Latif, S., Abbas, H. and Khan, F.A., 2018. Malicious insiders attack in IoT based multi-cloud e-healthcare environment: A systematic literature review. Multimedia Tools and Applications, 77(17), pp.21947-21965.

[21] Moustafa, N., 2021. A Systemic IoT–Fog–Cloud Architecture for Big-Data Analytics and Cyber Security Systems. Secure Edge Computing: Applications, Techniques and Challenges, p.41.

[22] Sailakshmi, V., 2021. Analysis of Cloud Security Controls in AWS, Azure, and Google Cloud.

[23] Moreno Alarcon, D.P., Vautier, J.F., Hernandez, G. and Guarnieri, F., 2019. Systems Thinking in Risk Management by Preventive & Detective Controls as an Ago-Antagonistic Systems Approach in the French Nuclear Sector. HAL.

[24] Suryateja, P.S., 2018. Threats and vulnerabilities of cloud computing: a review. International Journal of Computer Sciences and Engineering, 6(3), pp.297-302.

[25] Saravanan, A., Bama, S.S., Kadry, S. and Ramasamy, L.K., 2019. A new framework to alleviate DDoS vulnerabilities in cloud computing. International Journal of Electrical & Computer Engineering (2088-8708), 9(5).

[26] Zhu, G., Yin, Y., Cai, R. and Li, K., 2017, June. Detecting virtualization specific vulnerabilities in cloud computing environment. In 2017 IEEE 10th International Conference on Cloud Computing (CLOUD) (pp. 743-748). IEEE.

[27] Jalwa, S., Sharma, V., Siddiqi, A.R., Gupta, I. and Singh, A.K., 2021. Comprehensive and comparative analysis of different files using CP-ABE. In Advances in Communication and Computational Technology (pp. 189-198). Springer, Singapore.

[28] Zhang, M., Chen, Y. and Huang, J., 2020. SE-PPFM: A searchable encryption scheme supporting privacy-preserving fuzzy multikeyword in cloud systems. IEEE Systems Journal, 15(2), pp.2980-2988.

[29] Odun-Ayo, I., Ananya, M., Agono, F. and Goddy-Worlu, R., 2018, July. Cloud computing architecture: A critical analysis. In 2018 18th international conference on computational science and applications (ICCSA) (pp. 1-7). IEEE.

[30] Saha, O. and Dasgupta, P., 2018. A comprehensive survey of recent trends in cloud robotics architectures and applications. Robotics, 7(3), p.47.

[31] Al-Hujran, O., Al-Lozi, E.M., Al-Debei, M.M. and Maqableh, M., 2018. Challenges of cloud computing adoption from the TOE framework perspective. International Journal of E-Business Research (IJEBR), 14(3), pp.77-94.

[32] Bhushan, K. and Gupta, B.B., 2017. Security challenges in cloud computing: state-of-art. International Journal of Big Data Intelligence, 4(2), pp.81-107.

[33] Arora, P. and Dixit, A., 2018, December. Cloud Testing-Proposed Framework with its Scope, Importance, Methodologies, Challenges. In 2018 4th International Conference on Computing Communication and Automation (ICCCA) (pp. 1-4). IEEE.

[34] Abu-Darwish, N.J., Al-Kasasbeh, M.M. and Al-Khasawneh, M.M., 2021. The mediating role of cloud computing in the relationship between talent management and competitive advantages. Competitiveness Review: An International Business Journal.

[35] Abdalla, P.A. and Varol, A., 2019, June. Advantages to Disadvantages of Cloud Computing for Small-Sized Business. In 2019 7th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-6). IEEE.

[36] Ramya, K. Ruth, T. Sasidhar, D. Naga Malleshwari, and M. T. V. S. Rahul. "A review on security aspects of data storage in cloud computing." International Jounal of Applied Engineering Research 10, no. 5 (2015): 13383-13394.

[37] Moura, Jose, and David Hutchison. "Review and analysis of networking challenges in cloud computing." Journal of Network and Computer Applications 60 (2016): 113-129.

[38] Birje, Mahantesh N., Praveen S. Challagidad, R. H. Goudar, and Manisha T. Tapale. "Cloud computing review: concepts, technology, challenges and security." International Journal of Cloud Computing 6, no. 1 (2017): 32-57.

[39] AbdElmonem, Mohamed A., Eman S. Nasr, and Mervat H. Geith. "Benefits and challenges of cloud ERP systems–A systematic literature review." Future Computing and Informatics Journal 1, no. 1-2 (2016): 1-9.

[40] Sari, Arif. "A review of anomaly detection systems in cloud networks and survey of cloud security measures in cloud storage applications." Journal of Information Security 6, no. 02 (2015): 142.

[41] Sahmim, Syrine, and Hamza Gharsellaoui. "Privacy and security in internet-based computing: cloud computing, internet of things, cloud of things: a review." Procedia computer science 112 (2017): 1516-1522.

[42] Al-Shqeerat, H. A. K., F. M. Al-Shrouf, Mohammad R. Hassan, and HassenFajraoui. "Cloud computing security challenges in higher educational institutions-A survey." International Journal of Computer Applications 161, no. 6 (2017): 22-29.

[43] Shirazi, Syed Noorulhassan, AntoniosGouglidis, ArshamFarshad, and David Hutchison. "The extended cloud: Review and analysis of mobile edge computing and fog from a security and resilience perspective." IEEE Journal on Selected Areas in Communications 35, no. 11 (2017): 2586-2595.

[44] De Carvalho, Carlos André Batista, Rossana Maria de Castro Andrade, Miguel Franklin de Castro, Emanuel Ferreira Coutinho, and NazimAgoulmine. "State of the art and challenges of security SLA for cloud computing." Computers & Electrical Engineering 59 (2017): 141-152.

[45] Halabi, Talal, and Martine Bellaiche. "Towards quantification and evaluation of security of Cloud Service Providers." Journal of Information Security and Applications 33 (2017): 55-65.

[46] Ramachandra, Gururaj, MohsinIftikhar, and FarrukhAslam Khan. "A comprehensive survey on security in cloud computing." Procedia Computer Science 110 (2017): 465-472.

[47] Ouedraogo, Moussa, Severine Mignon, HerveCholez, Steven Furnell, and Eric Dubois. "Security transparency: the next frontier for security research in the cloud." Journal of Cloud Computing 4, no. 1 (2015): 1-14.

[48] Ardagna, Claudio A., RasoolAsal, Ernesto Damiani, and QuangHieu Vu. "From security to assurance in the cloud: A survey." ACM Computing Surveys (CSUR) 48, no. 1 (2015): 1-50.

[49] Pattakou, Argyri, Christos Kalloniatis, and StefanosGritzalis. "Security and privacy requirements engineering methods for traditional and cloud-based systems: a review." Cloud Comput 2017 (2017): 155.

[50] Halabi, Talal, and Martine Bellaiche. "A broker-based framework for standardization and management of Cloud Security-SLAs." Computers & Security 75 (2018): 59-71.

[51] Sheikh, Abdullah, Malcolm Munro, and David Budgen. "Systematic Literature Review (SLR) of resource scheduling and security in cloud computing." International journal of advanced computer science and applications. 10, no. 4 (2019).

[52] Jabbar, Jahangir, HussainMehmood, and Hassaan Malik. "Security of cloud computing: belongings for the generations." International Journal of Engineering & Technology 9, no. 2 (2020): 454-457.

[53] Al-Issa, Yazan, Mohammad Ashraf Ottom, and Ahmed Tamrawi. "eHealth cloud security challenges: a survey." Journal of healthcare engineering 2019 (2019).

[54] Tabrizchi, Hamed, and MarjanKuchaki Rafsanjani. "A survey on security challenges in cloud computing: issues, threats, and solutions." The journal of supercomputing 76, no. 12 (2020): 9493-9532.

[55] Mansouri, N., R. Ghafari, and B. Mohammad HasaniZade. "Cloud computing simulators: A comprehensive review." Simulation Modelling Practice and Theory 104 (2020): 102144.

[56] Jouini, Mouna, and Latifa Ben ArfaRabai. "Comparative study of information security risk assessment models for cloud computing systems." Procedia Computer Science 83 (2016): 1084-1089.

[57] Khan, MdAnit, Andrew Paplinski, Abdul Malik Khan, ManzurMurshed, and RajkumarBuyya. "Dynamic virtual machine consolidation algorithms for energy-efficient cloud resource management: a review." Sustainable cloud and energy services (2018): 135-165.

[58] Verma, Prabal, Aditya Gupta, and Rakesh Singh Sambyal. "Security Issues and Challenges in Cloud Computing: A Review." International Journal of Scientific Research in Computer Science, Engineering and Information Technology 4, no. 1 (2018): 1-4.

[59] Zhang, Q., Wang, X., Yuan, J., Liu, L., Wang, R., Huang, H., & Li, Y. (2019). A hierarchical group key agreement protocol using orientable attributes for cloud computing. *Information Sciences*, *480*, 55-69.

[60] Jiang, Q., Zhang, N., Ni, J., Ma, J., Ma, X., &Choo, K. K. R. (2020). Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles. IEEE Transactions on Vehicular Technology, 69(9), 9390-9401.

[61] Sharma, G., &Kalra, S. (2018). A lightweight multi-factor secure smart card based remote user authentication scheme for cloud-IoT applications. *Journal of information security and applications*, *42*, 95-106.

[62] Joseph, T., Kalaiselvan, S. A., Aswathy, S. U., Radhakrishnan, R., &Shamna, A. R. (2021). A multimodal biometric authentication scheme based on feature fusion for

improving security in cloud environment. Journal of Ambient Intelligence and Humanized Computing, 12(6), 6141-6149.

[63] Haseeb, K., Almogren, A., Ud Din, I., Islam, N., &Altameem, A. (2020). SASC: Secure and authentication-based sensor cloud architecture for intelligent Internet of Things. *Sensors*, *20*(9), 2468.

[64] Xu, J., Yu, Y., Meng, Q., Wu, Q., & Zhou, F. (2020). Role-Based Access Control Model for Cloud Storage Using Identity-Based Cryptosystem. Mobile Networks and Applications, 1-18.

[65] Veerabathiran, V. K., Mani, D., Kuppusamy, S., Subramaniam, B., Velayutham, P., Sengan, S., &Krishnamoorthy, S. (2020). Improving secured ID-based authentication for cloud computing through novel hybrid fuzzy-based homomorphic proxy re-encryption. Soft Computing, 24(24), 18893-18908.

[66] Benifa, J. B., & Mini, G. V. (2020). Modified Chebyshev polynomial-based access control mechanism for secured data access in cloud computing environment. Service Oriented Computing and Applications, 1-17.

[67] Anilkumar, C., & Subramanian, S. (2020). A novel predicate based access control scheme for cloud environment using open stack swift storage. Peer-to-Peer Networking and Applications, 1-13.

[68] Megouache, L., Zitouni, A., &Djoudi, M. (2020). Ensuring user authentication and data integrity in multi-cloud environment. Human-centric Computing and Information Sciences, 10(1), 1-20.

[69] Oyeyinka, I. F., Idowu, S., &Kuyoro, A. (2021). A symbolic attribute-based access control model for data security in the cloud. ITEGAM-JETIA, 7(29), 36-46.

[70] Fugkeaw, S., & Sato, H. (2018). Scalable and secure access control policy update for outsourced big data. Future Generation Computer Systems, 79, 364-373.

[71] Wang, J., Wang, H., & Zhang, H. (2020). A trust and attribute-based access control framework in internet of things. International Journal of Embedded Systems, 12(1), 116-124.

[72] Xue, K., Chen, W., Li, W., Hong, J., & Hong, P. (2018). Combining data owner-side and cloud-side access control for encrypted cloud storage. IEEE Transactions on Information Forensics and Security, 13(8), 2062-2074.

[73] Yadav, C., Patro, B. D. K., &Yadav, V. (2021). AES-Light Weight CP–ABE Based Privacy Protection Framework with Effective Access Control Mechanism in Cloud Framework. Design Engineering, 2321-2336.

[74] Chandel, S., Yang, G., &Chakravarty, S. (2020). AES–CP–IDABE: A Privacy Protection Framework against a DoS Attack in the Cloud Environment with the Access Control Mechanism. Information, 11(8), 372.

[75] Mahmood, G. S., Huang, D. J., & Jaleel, B. A. (2019). A secure cloud computing system by using encryption and access control model. Journal of Information Processing Systems, 15(3), 538-549.

[76] Eltayieb, N., Wang, P., Hassan, A., Elhabob, R., & Li, F. (2019). ASDS: Attribute-based secure data sharing scheme for reliable cloud environment. *Security and Privacy*, *2*(2), e57.

[77] Li, Y., Yu, Y., Yang, B., Min, G., & Wu, H. (2018). Privacy preserving cloud data auditing with efficient key update. Future Generation Computer Systems, 78, 789-798.

[78] Li, J., Zhang, Y., Chen, X., & Xiang, Y. (2018). Secure attribute-based data sharing for resource-limited users in cloud computing. Computers & Security, 72, 1-12.

[79] Ding, S., Li, C., & Li, H. (2018). A novel efficient pairing-free CP-ABE based on elliptic curve cryptography for IoT. IEEE Access, 6, 27336-27345.

[80] Challagidad, P. S., &Birje, M. N. (2020). Efficient multi-authority access control using attribute-based encryption in cloud storage. Procedia Computer Science, 167, 840-849.

[81] Tian, H., Li, X., Quan, H., Chang, C. C., & Baker, T. (2020). A lightweight attribute-based access control scheme for intelligent transportation system with full privacy protection. IEEE Sensors Journal.

[82] Xiong, S., Ni, Q., Wang, L., & Wang, Q. (2020). SEM-ACSIT: secure and efficient multiauthority access control for IoT cloud storage. IEEE Internet of Things Journal, 7(4), 2914-2927.

[83] Ding, S., Cao, J., Li, C., Fan, K., & Li, H. (2019). A novel attribute-based access control scheme using blockchain for IoT. IEEE Access, 7, 38431-38441.

[84] Yu, Y., Hu, L., & Chu, J. (2020). A secure authentication and key agreement scheme for IoT-based cloud computing environment. Symmetry, 12(1), 150.

[85] Belguith, S., Kaaniche, N., Laurent, M., Jemai, A., &Attia, R. (2020). Accountable privacy preserving attribute based framework for authenticated encrypted access in clouds. Journal of Parallel and Distributed Computing, 135, 1-20.

[86] Narayanan, U., Paul, V., & Joseph, S. (2020). A novel system architecture for secure authentication and data sharing in cloud enabled Big Data Environment. Journal of King Saud University-Computer and Information Sciences.

[87] Xu, Q., Tan, C., Fan, Z., Zhu, W., Xiao, Y., & Cheng, F. (2018). Secure multi-authority data access control scheme in cloud storage system based on attribute-based signcryption. IEEE Access, 6, 34051-34074.

[88] Panda, S. K., & Jana, P. K. (2019). An energy-efficient task scheduling algorithm for heterogeneous cloud computing systems. Cluster Computing, 22(2), 509-527.

[89] Zhang, X., Wu, T., Chen, M., Wei, T., Zhou, J., Hu, S., &Buyya, R. (2019). Energy-aware virtual machine allocation for cloud with resource reservation. Journal of Systems and Software, 147, 147-161.

[90] Alhassan, Sarah, and MajedAbdulghani. "A bio-inspired algorithm for virtual machines allocation in public clouds." Procedia Computer Science 151 (2019): 1072-1077.

[91] Bouterse, B., &Perros, H. (2019). Performance analysis of the reserve capacity policy for dynamic VM allocation in a SaaS environment. Simulation Modelling Practice and Theory, 93, 293-304.

[92] Bouterse, B., &Perros, H. (2018). Dynamic VM allocation in a SaaS environment. Annals of Telecommunications, 73(3), 205-218.

[93] Tarahomi, Mehran, Mohammad Izadi, and MostafaGhobaei-Arani. "An efficient power-aware VM allocation mechanism in cloud data centers: a micro genetic-based approach." Cluster Computing (2020): 1-16.

[94] Son, Jungmin, and RajkumarBuyya. "Priority-aware VM allocation and network bandwidth provisioning in software-defined networking (SDN)-enabled clouds." IEEE Transactions on Sustainable Computing 4, no. 1 (2018): 17-28

[95] Hanini, Mohamed, Said El Kafhali, and Khaled Salah. "Dynamic VM allocation and traffic control to manage QoS and energy consumption in cloud computing environment." International Journal of Computer Applications in Technology 60, no. 4 (2019): 307-316.

[96] Saxena, Deepika, and Ashutosh Kumar Singh. "A proactive autoscaling and energy-efficient vm allocation framework using online multi-resource neural network for cloud data center." Neurocomputing 426 (2021): 248-264.

[97] Zhang, P., Zhou, M., & Wang, X. (2020). An intelligent optimization method for optimal virtual machine allocation in cloud data centers. IEEE Transactions on Automation Science and Engineering, 17(4), 1725-1735.

[98] Zhang, X., Wu, T., Chen, M., Wei, T., Zhou, J., Hu, S., &Buyya, R. (2019). Energy-aware virtual machine allocation for cloud with resource reservation. Journal of Systems and Software, 147, 147-161.

[99] Rahmanian, A. A., Horri, A., &Dastghaibyfard, G. (2018). Toward a hierarchical and architecture-based virtual machine allocation in cloud data centers. International Journal of Communication Systems, 31(4), e3490.

[100] Rawat, P. S., Dimri, P., &Saroha, G. P. (2020). Virtual machine allocation to the task using an optimization method in cloud computing environment. International Journal of Information Technology, 12(2), 485-493.

[101] Jia, H., Liu, X., Di, X., Qi, H., Cong, L., Li, J., & Yang, H. (2019). Security strategy for virtual machine allocation in cloud computing. Procedia computer science, 147, 140-144.

[102] Qie, X., Jin, S., &Yue, W. (2019). An energy-efficient strategy for virtual machine allocation over cloud data centers. Journal of Network and Systems Management, 27(4), 860-882.

[103] Wang, X. S., Zhu, J., Jin, S. F., Yue, W. Y., & Takahashi, Y. (2019). Performance evaluation and social optimization of an energy-saving virtual machine allocation scheme within a cloud environment. Journal of the Operations Research Society of China, 1-20.

[104] Zaidi, R. T. (2018). Virtual Machine Allocation Policy in Cloud Computing Environment using CloudSim. International Journal of Electrical & Computer Engineering (2088-8708), 8(1).

[105] Xu, P., He, G., Li, Z., & Zhang, Z. (2018). An efficient load balancing algorithm for virtual machine allocation based on ant colony optimization. International Journal of Distributed Sensor Networks, 14(12), 1550147718793799.

[106] Omer, S., Azizi, S., Shojafar, M., &Tafazolli, R. (2021). A priority, power and traffic-aware virtual machine placement of IoT applications in cloud data centers. Journal of Systems Architecture, 115, 101996.

[107] Agarwal, A., & Duong, T. N. B. (2019). Secure virtual machine placement in cloud data centers. Future Generation Computer Systems, 100, 210-222.

[108] Fatima, A., Javaid, N., Anjum Butt, A., Sultana, T., Hussain, W., Bilal, M., ...&Ilahi, M. (2019). An enhanced multi-objective gray wolf optimization for virtual machine placement in cloud data centers. Electronics, 8(2), 218.

[109] Ponraj, A. (2019). Optimistic virtual machine placement in cloud data centers using queuing approach. Future Generation Computer Systems, 93, 338-344.

[110] Rani, S., &Suri, P. K. (2020). An efficient and scalable hybrid task scheduling approach for cloud environment. International Journal of Information Technology, 12(4), 1451-1457.

[111] Li, Fagen, Bo Liu, and Jiaojiao Hong. "An efficient signcryption for data access control in cloud computing." *Computing* 99, no. 5 (2017): 465-479.

[112] Ethelbert, Obinna, FarazFatemiMoghaddam, Philipp Wieder, and RaminYahyapour. "A JSON token-based authentication and access management schema for Cloud SaaS applications." In *2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud)*, pp. 47-53. IEEE, 2017.

[113] Gupta, B. B., and MeghaQuamara. "An identity based access control and mutual authentication framework for distributed cloud computing services in IoT environment using smart cards." *Procedia computer science* 132 (2018): 189-197.

[114] Wadhwa, Amit, and Vinod Kumar Gupta. "Proposed Framework with Comparative Analysis of Access Control & Authentication based Security Models Employed over Cloud." *International Journal of Applied Engineering Research* 12, no. 24 (2017): 15715-15722.

[115] Zhang, Qikun, Yongjiao Li, Zhigang Li, Junling Yuan, Yong Gan, and XiangyangLuo. "Access control based on ciphertext attribute authentication and threshold policy for the internet of things." *Sensors* 19, no. 23 (2019): 5237.

[116] Kappes, Giorgos, AndromachiHatzieleftheriou, and Stergios V. Anastasiadis. "Multitenant access control for cloud-aware distributed filesystems." *IEEE Transactions on Dependable and Secure Computing* 16, no. 6 (2017): 1070-1085.

[117] Joshi, Maithilee, Karuna Joshi, and Tim Finin. "Attribute based encryption for secure access to cloud based EHR systems." In *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, pp. 932-935. IEEE, 2018.

[118] Zhu, Huijun, Licheng Wang, Haseeb Ahmad, and XinxinNiu. "Key-policy attribute-based encryption with equality test in cloud computing." *IEEE Access* 5 (2017): 20428-20439.

[119] Xue, Shumin, and ChengjuanRen. "Security Protection of System Sharing Data with Improved CP-ABE Encryption Algorithm under Cloud Computing Environment." *Automatic Control and Computer Sciences* 53, no. 4 (2019): 342-350.

[120] Ming, Yang, Baokang He, and Chenhao Wang. "Efficient Revocable Multi-Authority Attribute-Based Encryption for Cloud Storage." *IEEE Access* 9 (2021): 42593-42603.

[121] Li, Yannan, Yong Yu, Bo Yang, Geyong Min, and Huai Wu. "Privacy preserving cloud data auditing with efficient key update." *Future Generation Computer Systems* 78 (2018): 789-798.

[122] Shen, Zhirong, JiwuShu, and Wei Xue. "Keyword search with access control over encrypted cloud data." *IEEE Sensors journal* 17, no. 3 (2016): 858-868.

[123] Zhou, Junwei, HuiDuan, Kaitai Liang, Qiao Yan, Fei Chen, F. Richard Yu, Jieming Wu, and Jianyong Chen. "Securing outsourced data in the multi-authority cloud with fine-grained access control and efficient attribute revocation." *The Computer Journal* 60, no. 8 (2017): 1210-1222.

[124] Balusamy, Balamurugan, P. Venkata Krishna, GS TamizhArasi, and Victor Chang. "A Secured Access Control Technique for Cloud Computing Environment Using Attribute Based Hierarchical Structure and Token Granting System." *IJ Network Security* 19, no. 4 (2017): 559-572.

[125] Namasudra, Suyel, Pinki Roy, PandiVijayakumar, SivaramanAudithan, and BalamuruganBalusamy. "Time efficient secure DNA based access control model for cloud computing environment." *Future Generation Computer Systems* 73 (2017): 90-105.

[126] Namasudra, Suyel, RupakChakraborty, AbhishekMajumder, and Nageswara Rao Moparthi. "Securing Multimedia by Using DNA-Based Encryption in the Cloud Computing Environment." *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)* 16, no. 3s (2020): 1-19.

[127] Wadhwa, Amit, and Vinod Kumar Gupta. "Proposed Framework with Comparative Analysis of Access Control & Authentication based Security Models Employed over Cloud." *International Journal of Applied Engineering Research* 12, no. 24 (2017): 15715-15722.

[128] Prince, P. Blessed, and SP JenoLovesum. "Privacy enforced access control model for secured data handling in cloud-based pervasive health care system." *SN Computer Science* 1, no. 5 (2020): 1-8.

[129] Shen, Rui, and Xuejun Zhu. "The Research on Multi-Authority Based Weighted Attribute Encryption Algorithm in the Cloud Computing Environment." In *4th International Conference on Computer, Mechatronics, Control and Electronic Engineering*. Atlantis Press, 2015.

[130] Wang, Shulan, Kaitai Liang, Joseph K. Liu, Jianyong Chen, Jianping Yu, and WeixinXie. "Attribute-based data sharing scheme revisited in cloud computing." *IEEE Transactions on Information Forensics and Security* 11, no. 8 (2016): 1661-1673.

[131] Zhang, Wenfeng, and Shiqi Jin. "Research and Application of Data Privacy Protection Technology in Cloud Computing Environment Based on Attribute Encryption." In *2020 IEEE International Conference on Power, Intelligent Computing and Systems (ICPICS)*, pp. 994-996. IEEE, 2020.

[132] Qian, He, Song Jing, Xu Hong, and Wang Yong. "HABEm: Hierarchical Attribute Based Encryption with Multi-Authority for the Mobile Cloud Service." In *2020 IEEE/CIC International Conference on Communications in China (ICCC)*, pp. 524-529. IEEE, 2020.

[133] Chaudhry, Shehzad Ashraf, HosamAlhakami, Abdullah Baz, and Fadi Al-Turjman. "Securing demand response management: A certificate-based access control in smart grid edge computing infrastructure." *IEEE Access* 8 (2020): 101235-101243.

[134] Muthurajkumar, Sannasy, MuthuswamyVijayalakshmi, and ArputharajKannan. "Secured data storage and retrieval algorithm using map reduce techniques and chaining encryption in cloud databases." *Wireless Personal Communications* 96, no. 4 (2017): 5621-5633.

[135] Alam, Masoom, Naina Emmanuel, Tanveer Khan, Yang Xiang, and HoucineHassan. "Garbled role-based access control in the cloud." *Journal of Ambient Intelligence and Humanized Computing* 9, no. 4 (2018): 1153-1166.

[136] Goyal, V.; Pandey, O.; Sahai, A.; Waters, B. Attribute-based encryption for fine-grained access control of encryption data. In Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS 2006, Alexandria, VA, USA, 30 October–3 November 2006; pp. 89–98.

[137] Jain, Raj. "Advanced encryption standard (AES)." *Washington University in Saint Louis, St. Louis* (2017).