DESIGN OF NOVEL TECHNIQUE FOR OPTIMIZING SECURITY IN PUBLIC CLOUD STORAGE

A Thesis submitted

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY
IN
COMPUTER SCIENCE AND ENGINEERING

By

G NAGARAJAN
17SCSE301034

Supervisor

Dr. SAMPATH KUMAR K
Professor

SCHOOL OF COMPUTING SCIENCE & ENGINEERING
GALGOTIAS UNIVERSITY
Plot No 2, Sector 17-A Yamuna Expressway
Greater Noida, Uttar Pradesh
INDIA

NOVEMBER, 2021

CANDIDATE DECLARATION

I hereby certify that the work which is being presented in the thesis, entitled " **DESIGN OF NOVEL TECHNIQUE FOR OPTIMIZING SECURITY IN PUBLIC CLOUD STORAGE**" in partial fulfillment of the requirements for the award of the degree of Doctor of Philosophy in Faculty of Computer Science and Engineering and submitted in Galgotias University, Uttar Pradesh is an authentic record of my own work carried out during a period from January 2018 under the supervision of **Dr. SAMPATH KUMAR K**, Professor, School of Computing Science and Engineering, Galgotias University.

The matter embodied in this thesis has not been submitted by me for the award of any other degree or from any other University/Institute.

G NAGARAJAN
17SCSE301034

This is to certify that the above statement made by the candidate is correct to the best of our knowledge.

Dr. SAMPATH KUMAR K
Supervisor
SCSE

School of Computing Science & Engineering
Galgotias University

CERTIFICATE

This is to certify that **Mr. G NAGARAJAN (Reg. No.17SCSE301034)** has presented his pre-submission seminar of the thesis entitled **"DESIGN OF NOVEL TECHNIQUE FOR OPTIMIZING SECURITY IN PUBLIC CLOUD STORAGE"** before the committee and summary is approved and forwarded to School Research Committee of of Computing Science & Engineering, in the Faculty of Engineering & Technology, Galgotias University, Uttar Pradesh.

Dean – SCSE Dean – PhD & PG

The Ph.D. Viva-Voice examination of **G NAGARAJAN** Research Scholar, has been held on _____

Supervisor External Examiner

APPROVAL SHEET

This thesis/dissertation/report entitled "**DESIGN OF NOVEL TECHNIQUE FOR OPTIMIZING SECURITY IN PUBLIC CLOUD STORAGE"** by **G NAGARAJAN** is approved for the degree of Doctor of Philosophy.

Examiner Supervisor Chairman

ACKNOWLEDGEMENT

Working as an Assistant Professor and doing research for the degree of Ph.D in Galgotias University was quite magnificent and challenging experience for me. In all these years, many people directly or indirectly contributed in shaping up my career. It was hardly possible for me to complete my doctoral work without the precious and invaluable support of these personalities.

I would like to give my small tribute to all those people. Initially, I would express my sincere gratitude to my supervisor Dr.SAMPATH KUMAR K Professor, School of Computing Science and Engineering for his valuable guidance, enthusiasm and overfriendly nature that helped me a lot to complete my research work in a timely manner.

I must owe a special debt of gratitude to Hon'ble Chancellor Mr. Suneel Galgtotia, Mr. Dhruv Galgotia, CEO and Hon'ble Vice-Chancellor Dr. Preeti Bajaj, Galgotias University for their valuable support throughout my research work.

I express my sincere thanks to Dr. Munish Sabharwal, Dean School of Computing Science & Engineering and Dr.Naresh Kumar, Dean PG & PhD for their guidance and moral support during my research work and all faculties of School of Computing Science & Engineering who helped me a lot in my course of research work and all those who stood behind me.

Nothing is possible without the constant support of my family. I would like to convey my deep regard to my parents for their wise counsel and indispensable advice that always encouraged me to work hard for the completion of my research work. My highest gratitude goes to my parent's and all my family members for their relentless support, blessings and encouragement. Special mention goes to my wife, M Rama, and my kids, N Koushik Darshan and N Liashini; my final thanks to all my friends and those who stood behind me like support and helped me complete this dissertation.

G. NAGARAJAN

ABSTRACT

Cloud computing (CC) technologies effectively utilize existent physical resources through virtualization, allowing many users to use a common underlying physical infrastructure in a distributed environment. It is possible to provide dispersed, scalable and dynamic computational resources to clients via the high-speed online platform by using the ideas of cloud computing. The demand for cloud services is continuously increasing due to the limited resources available for storing data in the local environment. Along with this, the necessity for information security in cloud environments is becoming more apparent as another critical duty to do. The information security in cloud storage is based not only on the significance of the service provider but also on confidence maintained by an individual user who is all accessing the information from cloud storage. Many of the researcher consider the conventional encryption technique for making the information confidentiality for maintain the security through public key encryption techniques.

But still the information shared among the users through the cloud storage is the challenging one. From the view of users, the cloud appears as a single point of access for all their expected computing needs. Cloud technology enables users to store their data remotely and to access cloud applications on demand without the need for on-premises hardware or software infrastructure. Still, data honesties and privacy are significant risks in a public cloud environment. Hence, there is a necessity to expand data security while maintaining the data in a public cloud.

To overcome these scenarios, the new scheme is proposed in this thesis with low computational complexity for secure information storage using attribute-based encryption technique with Monarchy Butterfly Optimization Algorithm. In cloud scenario, many security principles are implemented to maintain the secure transformation of data over the internet. And still, the main concern is maintaining the integrity of our data in the public cloud. The majority of research focuses on cryptographic solutions for safe data exchange. In the fourth phase of work, The MBO-ABE approach has been suggested because standard public-key encryption techniques are used to provide data secrecy, but it is unlikely to result in improved data sharing.

Additionally, attribute-based encryption (ABE) is being developed as a crucial approach to providing security while also establishing good data transfer in a parallel manner, both of which are important. The ABE is a well-known cryptographic mechanism used to save the user's private information in CC. Nevertheless, it is not practical to utilize it in cloud storage due to the complexity and the possibility of decryption key leaks. Therefore, a unique monarch butterfly optimization with attribute-based encryption (MBO-ABE) is developed to protect public cloud storage.

The MBO-ABE approach that has been provided is intended to store data safely in public cloud storage. ABE goal is to keep sensitive data private in public cloud storage by using ABE. Using the MBO method, which is based on the movement of monarch butterflies, it is possible to improve the security performances of the ABE approach by incorporating it into it. A significant number of scenarios are implemented to demonstrate the increased efficiency of the MBO-ABE approach that has been provided. The experimental results demonstrated that the MBO-ABE methodology outperformed all other current techniques, and the MBO-ABE technique offered the highest level of performance.

The fifth phase of the research work inspects the improvement in the integrity and secure data transfer based on the Parallel Chunk Encryption (PCE) Scheme, which inspects the reliability of the information in the public cloud with the cooperation of Trusted Third-Party Auditor (TTPA). The document holder chops the file (documents, videos. etc.) into multiple chunks. Every chunk encrypted using the Parallel Chunk Encryption (PCE) scheme and, Forward Encipher (FE) technique. The proposed Forward Encipher technique forwards the encrypted chunk to carry out the next chunk encryption is necessary to perform the XOR operation in every chunk encryption it constructs to strengthen the confidentiality of data. PCE reduces the encryption time for chunks in a massive amount of size. In terms of data share and storage in a public cloud environment, the proposed PCE scheme could be more efficient and secure in considerable time.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AAC - Attribute Audit Center

ABS - Attribute-Based Signature

ABE - Attribute Based Encryption

ACE - Asymmetric Convergent Encryption

AES - Advanced Encryption Standard

AGC - Authenticators Generation Center

API - Application Programming Interface#

AWS - Amazon Web Service

BH-WABE - Blowfish Hybridized -Weighted Attributed Base Encryption

BUG - Bottom-Up Generalization

CBO - Confidentiality enabled Obfuscation

CBC - Cipher Block Chaining

CC - Cloud Computing

CCA - Chosen-Ciphertext Attacks

CP-ABE - Cipher text Policy Attribute Based Encryption

CRM - Customer Relationship Management

CSP - Cloud Service Provider

CSNET - Computer Service Network

DaaS - Data and Database Services

DES	-	Data Encryption Standard
DFA	-	Deterministic Finite Automata
DIA	-	Data Integrity Auditing
EEA	-	Enhanced Encryption Algorithm
HE	-	Honey Encryption
HABE	-	Hierarchical Attribute-Based Encryption
KGC	-	Key Generation Center
IAM	-	Identity and Access Management
IaaS	-	Infrastructure as a Service
IBET	-	Identity-based Encryption Transformation
IBBE	-	Identity-Based Broadcast Encryption
IBC	-	ID-Based Cryptography
IDEA	-	International Data Encryption Algorithm
IT	-	Information Technology
MBO	-	Monarchy Butterfly Optimization
MHT	-	Merkle Hash Tree
MuR-DPA-		Multi-Replica Dynamic Public Auditing
mCL-PKE-		mediated Certificateless Public Key Encryption
MV-PDP	-	Mutually Verifiable Provable Data Possession
NIST	-	National Institute of Standards and Technology

PaaS	-	Platform as a Service
PC	-	Public Cloud
PCE	-	Parallel Chunk Encryption
PDP	-	Proof of Data Ownership
PK	-	Public Key
PKG	-	Public Key Generation
POR	-	Proof of Retrievability
RSA	-	Ron Rivest Adi Shamir Algorithm
RRA	-	Related Randomness Attacks
SaaS	-	Software as a Service
SCSK	-	Storage Cost of Secret Key
SEA	-	Symmetric Encryption Algorithm
SLA	-	Service Level Agreement
SOA	-	Service Oriented Architecture
SOAP	-	Simple Object Access Protocol
SOC	-	Security Operation Center
SPAD	-	Secure Public cloud Storage Audit
SSA	-	Security Service Algorithm
SSH	-	Secure Shell
S3	-	Simple Storage Service

TPA	-	Third Party Auditor
TTPA	-	Trusted Third Party Audit
TOD	-	Tagging of Outsourced Data
VM	-	Virtual Machine
UKGT	-	User Key Generation Time

CHAPTER 1

INTRODUCTION

1.1 OVERVIEW OF A PROBLEM AND ITS MOTIVATION

Computing is an emerging specialized area with a Service-Oriented Architecture with a majority of Cloud services. The number of security problems and bugs in Public Cloud Storage also increased. This public cloud storage, also known as "storage-as-a-service" or online storage, is a service model that provides storage space on a charge basis to the general public. It is similar to how a public resource such as electricity or gas offers and charges for utilities. Public cloud selection requires third-party provider assistance to provide a variety of internet resources. Now, as it seems, there are no enough security protections in a public cloud. Over the years, public cloud providers' security mechanisms have been modified and developed to handle only sophisticated threats.

National Institute of Standards and Technology (NIST) claimed that cloud computing is a user-friendly framework to deliver services. Cloud technology provides services on user demand and allows users to use the network for distributed computing resources. Computer infrastructure may consist of "networks, servers, storage, applications, and service" with much less effort to manage them rapidly. The cloud infrastructure necessitates less communication with the cloud service provider [1]. NIST distinguishes Cloud Infrastructure influence of 4 deployment models of "public, private, hybrid, and community" [2][3] . The service models defined by NIST are SaaS, PaaS, and IaaS are among[4]. Cloud storage is a model infrastructure that maintains, manages, and backs up data from a remote location and makes data accessible to network users. It has a broader data center with a pool of several thousand machines and servers. Cloud delivers secure services to the users of numerous data centers in different places around the globe. Without human interference, it offers unrestricted service provisioning. The most important thing for cloud computing is information security and integrity, the Outsourced Data managed and tracked by the CSP [5]. There is an extensive assortment of ways to attack the information in the Public Cloud [6]. Outsourcing data brings cloud protection problems when moving to servers.

Once information is deployed to the cloud, CSP can only hold, track, and handle data presently used by many organizations and companies. public cloud storage is a public circumstance in which customer data can be hacked in several ways. An external CSP may maintain the data outsourced to the cloud. By thereby limiting the entry and exit points for data in and out of the cloud, and via the use of strict data protection rules such as confidentiality, availability, and transparency, users may be confident that their data is safe [5][7]. Cryptography is a powerful method for protecting data from unwanted access when data is on the cloud server. Cryptography is a word that refers to a data transmission system that restricts access to data to those who are authorized to read and process it, as well as a way of encrypting and decrypting data that includes both predictable and public-key cryptographic methods.

Traditional encryption, also known as symmetric key encryption, is distinguished by the fact that it employs the same symmetric key including both encryption / decryption operations. Using two keys to encrypt and decrypt data is known as Asymmetric Key Encryption(AES)[8]. The public cloud essential purpose is to allow the general public to store data and applications, and this is the cloud computing paradigm most commonly used.

Cloud service providers use the Internet to make services like infrastructure, computing, and servers accessible to enterprises. Third-Party distributors buy, manage and sell standard physical hardware as needed. Internet-based public cloud storage services are growing fast because they offer consumers significant cost savings and accessibility. In general, public cloud infrastructure offers advantages in data protection. It has significant benefits over conventional storage solutions includes Availability, Quick Disaster Recovery, automated software upgrades, Capital Expenditure Free, Costs-saving, No more maintenance Headache, Datacenter option, etc. Despite the challenging obstacle called data protection, considering the lack of openness of information sharing privacy in the cloud.

However, these public cloud storage services also pose possible safety threats when publicly available shared technology. Cloud computing networks, including hybrid clouds and group clouds, used in other types of multi-tenancy clouds, are often subject in reality to higher threats than private clouds.

Except in the private cloud, cloud infrastructure is almost definitely handled and run by a service provider off-premises to optimize the advantages of cloud computing. Off-premises storage is required for cloud storage use, such as disaster recovery backup. If data is no longer collected and handled on the property of the data owner, the data owner loses control over their data. As a result, cloud storage protection is problematic regardless of the implementation model if the service providers are not trusted [9].

It is necessary for cloud computing to use encrypted storage to protect the information of the data owner before it is stored in the cloud. With the assistance of a TPA, the accuracy of the information cache is ensured. Third-Party Auditor(TPA) is the protected Auditor, who must fulfil the two basic requirements. TPA can effectively track the Cloud information storage without needing local data and should not place unnecessary online burdens on cloud users. 2) No new threats to consumer privacy can be identified in the third-party audit process [10].

The public auditing framework must require cloud data storage so that consumers can use unbiased third-party auditors to audit outsourced data to protect transparency and save online processing costs thoroughly and electronic pressure. TPA that has the proficiency and the ability to track the integrity of all cloud-based information on behalf of customers daily is not feasible.

This help users to make their cloud storage both faster and more economical [11][12]. In response to the rapid rise of cloud computing and cloud storage, individual users and businesses are increasingly interested in outsourcing their data to distant storage facilities. This offers huge benefits to the data owners and the benefits are listed below.

- Users are relieved from the burden of maintaining the data in house.
- The user does not need to invest on the machines to expand the storage.
- It minimizes the capital expenditure of industries and they need to incur only operating expenses on their side.
- Users may access and handle data from any location at any time.

1.2 CLOUD-COMPUTING

Cloud technology is a web-based layout that gives on-trade applications to customers to reach the shared resource group, including software or hardware. The distributed computation considers the "Everything as a Service" model in both academic and modern networks. Both corporations and scientists/researchers are turning to cloud computing to store vast amounts of data rather than maintaining or creating their own local data centers due to cloud computing's development. Cloud systems are sold throughout the world today in the same manner as water and power services. As much as you have used these resources, you have to pay. Cloud consumers get various forms of Open Cloud computing resources [13].

The users now concentrate on their primary goal without caring about the need for computing resources. Over time, cloud storage capabilities are continuously increasing, and computing resources are becoming more effective. To provide the customer with dangerous accessible facilities, the quality that contributes to further improvement in the production must be increased [14]. In Figure 1.1: the cloud computing architecture consists of two models. It is necessary for every layer the model of fundamental resources obtained by the customer from the cloud architecture.

1.2.1 Cloud Computing Origin

Cloud computing knowledge has just been present for the recent decades; this is not known when cloud computing first emerged in the computer world. In science, the term "Cloud" is often used to refer to clusters of things that visually resemble a foggy sky. This was claimed to be a straightforward case of a long-running programme building a network around icons of servers and cluster network diagrams with overlapping circles that resembled clouds. For instance, the cloud was used as a symbol while describing the Internet.

Over time, it was adopted as a symbol for the Internet in computer networks, and it is still in use today. With these essential items, the inference is that how a network's endpoints communicate with one another is not essential to understanding the diagram. At the beginning of Arpanet, in early 1977, the cloud symbol represented networks of computer equipment.

The Computer Service Network (CSNET), which was created in 1981, and the Internet were both considered to be forerunners of an Internet. The term cloud has been used to refer to platforms for distributed computing. In April 1994, "Bill and Andy's Excellent Adventure II" on the Apple spin-off General 3 Magic, Andy Hertzfeld mentioned on General Magic's distributed programmable language. Many people have called the technology behind distributed computing a "cloud," but this word has also been used to describe other computing-in-the-cloud technologies.

The attractiveness of Telescript is that it allows for a single application to make use of all the Cloud's resources, where a virtual service could be created that has never been done before. Ideas of time-sharing and cloud computing became acquainted with each other in the early 1960s. It is often associated with well-known corporate figures like "*IBM and DEC*". Customers submitted their tasks to the operational manager, which then executed them on IBM mainframes, and this model was utilized to serve them in the data center. Companies that supply dedicated point-to-point data circuits offered VPN services at a cheap cost and delivered excellent levels of service quality by the late 1990s. After a while, they started to utilize the cloud symbol to signify the boundary between service providers' responsibility to their clients and end-user's obligation to use the service. Cloud computing broadened the scope of this advantage to include all servers as well as network equipment.

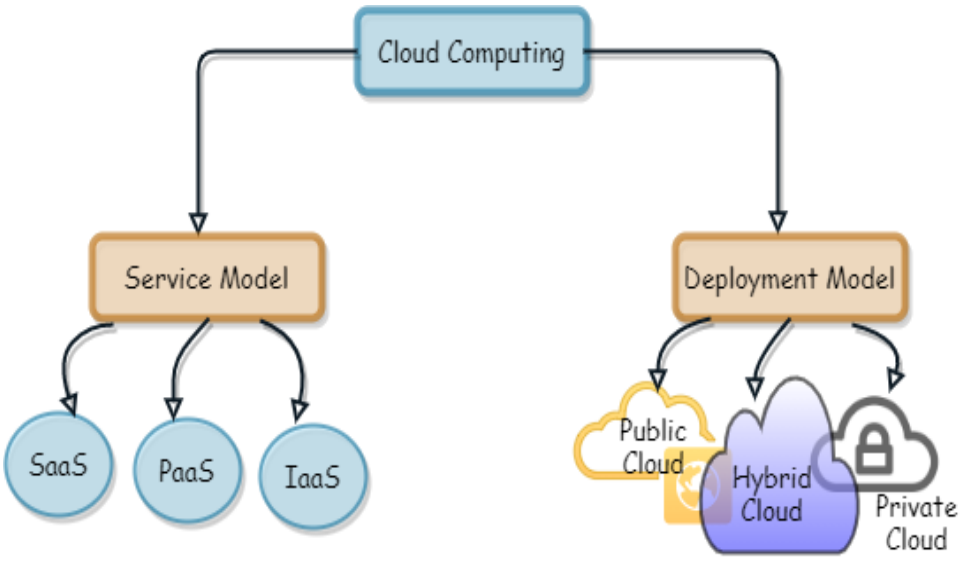

Figure 1.1 Cloud Computing Models

Computer scientists and engineers have come up with various approaches to making large-scale computer power more accessible to a more significant number of people via time-sharing. To enhance the infrastructure and platform, they performed tests with different algorithms. Application developers have been working on improving the efficiency of end-user's CPUs since 2000 when the first apps were created. Cloud computing became a reality in initial 2008, when "NASA's Open Nebula "software which was developed as part of the "RESERVOIR European Commission-funded" project, developed the first publicly available software for building private cloud and hybrid cloud, as well as federated cloud infrastructures. In the same year, they offer quality of service assurances to cloud-based foundations as part of the "IRMOS European Commission-supported project skeleton," which was sponsored by the Council of Europe. This happens in a real-time cloud environment and is supported by the company. Gartner stated in 2008 that cloud computing strengthens the allows users to connect information technology services and those who provide those services and that businesses are increasingly shifting away from enterprise-owned hardware and software resources toward charge service prototypes. In order to achieve the anticipated shift to computing, IT products will see spectacular growth in specific sectors while seeing a substantial decline in others due to the projected transition to computing.

Amazon launched the Elastic Compute Cloud in August 2006. "Microsoft Azure was first launched in October 2008 as 'Azure' and released as Windows Azure on February 1, 2010, before being renamed Microsoft Azure on March 25, 2014". Azure briefly appeared on the TOP500 list of supercomputers before being dropped. In July 2010, Rack space Hosting and NASA announced the introduction of Open Stack, an open-source cloud computing software project.

The Open Stack project's objective is to assist companies that provide cloud computing services using commodity hardware. The first code was built using NASA's Nebula and Rackspace's Cloud Files platforms. IBM launched the IBM Smart Cloud architecture on March 1, 2011, to create Smarter Planet. Cloud computing is a crucial component of Smarter Computing. Oracle announced the Oracle Cloud on June 7, 2012. The Oracle Cloud is still in its early phases; this cloud contribution is the first to provide clients with a unified set of IT solutions across the service models.

1.3 ARCHITECTURE OF CLOUD COMPUTING

As a logical evolution and adoption of existing technology and ideas, cloud computing is still considered to be in its early stages of development. The figure 1.2 illustrates the cloud architecture with its many service models. Cloud computing aims to enable consumers to use all of these technologies without requiring in-depth knowledge or experience in any of them. It is claimed that cloud computing would save expenses while allowing customers to concentrate on their main business rather than on IT limitations. Cloud computing is mainly made possible through virtualization, which is the most important technological enabler.

Virtualization software partitions a real computer into one or more "virtual" computers. It is possible to effectively use and manage these components to perform computing operations on the actual computer hardware.

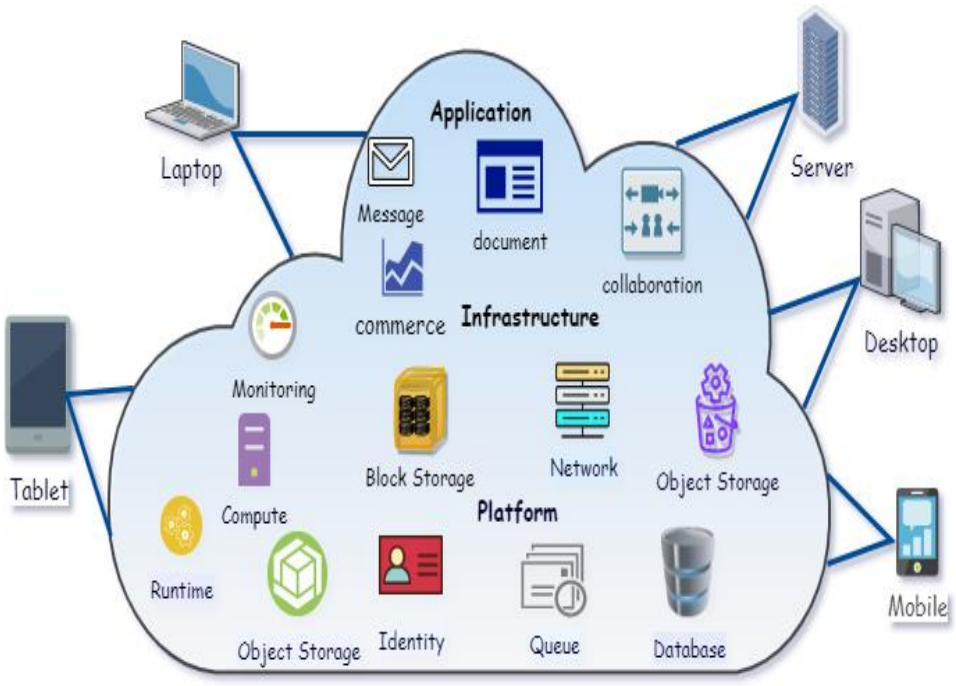

Figure1.2 Cloud Computing Architecture

Virtualization at the operating system level creates a distinct container that may be utilized independently of any existing computing devices; idle computer resources are effectively allocated and utilized. Virtualization offers the agility needed to speed up IT processes while also lowering costs by increasing the use of existing equipment.

In autonomous computing, the user's ability to create resources on-demand is simplified. Automation of processes accelerates the method, decreases labor charges, and diminishes the risk of user-initiated mistakes. Customers frequently face complicated business challenges, cloud computing includes aspects of Service-Oriented Architecture (SOA), which may assist customers in converting these roadblocks into services which may be combined to deliver a result to their problem(s). Cloud computing delivers all of its resources in the form of services. It leverages existing metrics and best practices from SOA to provide standardized access to cloud services to individuals worldwide in an informal and global environment. Cloud computing incorporates ideas from utility computing to track the usage of services. Pay-per-use models for public clouds are based on metrics, which are essential to their functioning. Regular servicing is also an essential component of self-repair systems, providing dynamic cooperation without limitation. Cloud computing, a subset of grid computing, evolved to address QoS (Quality Of Service) and security concerns [15] . Compared to conventional parallel computing methods, cloud affords the resources and software required to shape content equivalent applications at a lower cost.

1.4 CLOUD COMPUTING SERVICE MODELS

Even though SOA refers to "everything as a service," CSP offer their best "services" under diverse model types. The three models NIST uses are as follows: SaaS, IaaS, and PaaS, all of which are shown in Figure 1.3. Models are increasingly abstracted, with layers placed on top of one other in a stack, consecutively on a platform, and accessible via SaaS.. The fact is that they do not necessarily have to be connected. Furthermore, SaaS (Software as a Service) may be offered using actual servers (without running any PaaS or IaaS layers) since this approach allows for the bare-metal implementation of SaaS. On the contrary, a programme may be executed on IaaS and then accessed directly without the need to encapsulate it in a SaaS container. The layers of a cloud computing service model are organized in the stack structure. The following are the service models identified under the NIST Cloud Computing definition:

- Infrastructure as a Service
- Platform as a Service
- Software as a Service

Figure 1.3 Cloud Computing Service Model

1.4.1 Infrastructure as a Service

In contrast to conventional hardware machines, which need specific maintenance and have limited flexibility, this service model offers computer infrastructure to consumers and companies in order to enable virtualized computers. Cloud computing makes these devices practically accessible via the internet, with customizable specs and enhanced performance that are optimized for the customer's particular requirements, without requiring extra maintenance or limiting flexibility. Developers may install and operate the platforms required for software development. Additionally, this service enables the client to establish an instance for his desired virtual machine quickly and anyone can construct virtual machines for free or for a cheap cost in most cloud services. A straight virtual machine requires a hypervisor that operates on top of the kernel to be effective at virtualization. In comparison, containerization does not need a hypervisor, which increases processor efficiency and speed. Additionally, container sizes are variable, meaning they may be adjusted dynamically, eliminating the need for over-provisioning.

The most common way of using virtual machines is via providing objects, load balancers, or disc images. Those virtual machines will then be allocated unique IP addresses, thus protecting their identity in the cloud. These virtual counterparts are pre-configured on massive pools of hardware known to as data centers, which house them. The service providers charge for these virtual machines on a utility computing basis. The OS images and the application software need to be installed to deploy the applications to the cloud four infrastructure. It is the user's responsibility to patch up, update or maintain the operating system and the application software that they install. The provider will bill for the computing hour based on the usage and the number of resources allocated and utilized per the Service Level Agreement (SLA).

Users can set up a Windows server with a Linux Virtual Machine and change their plan and requirements as per their usage and demand. Users are only charged for what they use. With the help of this model, the industries or organizations infrastructure needs can be easily scaled up or down.

IaaS may provide the following basic virtual components:

1. Hardware of Computer system
2. Network of computers
3. The availability of internet access
4. Running client-specified virtual machines.
5. SLAs (Service level agreements)

Some of the advantages of IaaS are as follows:

- The delivery of efficient IT services is made easier when the environment is easily accessible and customized to the needs of each client.
- Maintenance, such as software upgrades and the most recent versions, is easily accessible through the internet.
- Lowers the expense of hardware maintenance, which may be very high.
- The virtual machine's data is secure and retrievable in the case of a host allocation failure.
- Can handle a large number of virtual instances based on demand.

1.4.2 Platform as a Service

This service architecture allows web application development and deployment. The whole software development life cycle is supported on-site at no extra expense. This service provides the client with a computer platform, which may include an operating system, programming platforms, web servers, databases, and other components. The fact that everything is done via the internet means that there is no need to be concerned about infrastructure or the bare minimal needs for the platform. The concern about incompatibility of software environments on machines may be eliminated with this approach, since the cloud service provider meets the hardware requirements needed by the platform directly, resulting in enormous and limitless computing capacity. Now, anybody with access to the internet can create strong and efficient apps without having to worry about infrastructure or cost problems. Traditional on-premise versions were costly and complicated, requiring a specialized set of hardware and software requirements to be met before they could be used. For each system need, there is a unique business solution that is created for it. Every combination of system requirement must be explicitly designed for the situation. This scenario used to compel the developers to make minor changes to the programme on a regular basis. In addition, massive amounts of energy were needed to keep the gear running.

Cloud-based application development has become more efficient, quicker, and more cost-effective as a result of the introduction of the PaaS paradigm. PaaS offers infrastructure, as well as the workflow tools, that are needed in the software development process. As part of its software development offerings, it also offers application services such as security, storage, database integration, instrumentation, and other similar services. Another feature of PaaS models is the ability to integrate online and mobile apps and services with databases via the use of the SOAP [16].

PaaS comprised of 3 fundamental components:

Stack - containing all middleware integration components, such as the speech virtual machine, servers, databases, data centers, and memory management mechanisms, among others.

Deployment Machinery - It is comprising of scripts and services for internet deployment of created apps.

User Experience -Each component of the frontend is provided, including the user interface, abstractions suited to particular requirements, and the ability to choose between several contexts.

Advantages of PaaS are:

- Agile apps may be developed and deployed with ease.
- Can concentrate on most essential resources for business without being distracted by concerns about the expense of the infrastructure.
- A PaaS provider's platforms are constantly updated, enabling developers to use the latest technologies.
- Increases productivity and reduces development time.
- Does not need the developer to be familiar with the backend operations of the cloud platform environment.
- Increase capacity as quickly as possible during peak periods and reduce power as required.
- Employees may log in and work on applications from any location.

1.4.3 Software as a Service (SaaS)

This method includes apps that are necessary for doing business. Access to the application is possible via a variety of devices, including web browsers and mobile phones. It is the cloud provider's infrastructure that these apps are operating on. Everything is managed by the service provider, including infrastructure, firewalls, operating systems, load balancers, a runtime environment for the applications, and a Customer Relationship Management system (CRM system) (CRM - ex: e-mail).

The provider is responsible for the cloud infrastructure's fundamental components, that include the network, storage, server, and operating system. The user is relieved of the responsibility of maintaining infrastructure on their own. The users are in charge of configuring the application's User-based, user-specific parameters.

However, ones it comes to SaaS, well-defined and formed information is provided to the user, which may be customized to a certain degree. SaaS services are provided to consumers via web browsers, allowing them to customize their experiences readily. Some SaaS services are also offered via Application Programming Interfaces (APIs), and developers may use these APIs to modify specific aspects of the service.

In the context of CC architecture, multi-tenancy is essential to success. On the webserver, just a single instance of the programme or application is running. This instance is made available to several clients, each of whom is referred to as a tenant. Multi-tenancy architecture is the term used to describe this kind of design. Virtual partitions are created on the server space of the service providers, and many tenants share this space.

Each user will have a visual representation of how they will interact with their instance, and the users will have the ability to modify the instance's characteristics. The most significant benefit of utilizing SaaS is that there is no need for an initial investment in servers, software, or license. A single instance of the programme may serve many clients, and the application developer is solely responsible for the maintenance of this one instance. Microsoft office 365 is a service provided by Microsoft that is an example of a SaaS provider. This service provides online access to Microsoft share point, Microsoft exchange point, Microsoft Lync, and Microsoft Office programmes. The key features are also accessible on their premises, and these services are provided as on-demand and hosted apps, respectively. These kinds of services provide a consistent user experience to the business across various devices and platforms[17].

Some of the advantages of IaaS are as follows:

1. Software that is easy to obtain reduces the time required to develop an application.
2. Improves the availability of applications globally.
3. System security and interoperability across the company/business.
4. The service providers are responsible for updating SaaS software.
5. Scale a solution easily to meet changing demands.
6. It doesn't need to be installed, updated, or managed in a typical way.

1.5 CLOUD DEPLOYMENT MODELS

Cloud service deployment types define the distinct category of the cloud environment and are primarily differentiated by the ownership, scale, and access they provide to customers. It includes information on the cloud's purpose and characteristics. Most businesses are eager to adopt cloud computing since it lowers capital investment while also controlling operational costs. Understanding the four deployment models is essential to choose which one best suits your website's needs.

1.5.1 Public Cloud

Services delivered through an open system qualify as "public cloud." Figure 1.4 depicts free public cloud services. Overall, there can be little variation among public and private cloud design; but even so, the safety considerations of various services (apps, storage and infrastructure) that are accessible to the public by a CSP and when communications are carried out over a network that is not trusted. CSP such as "*Amazon Web Services (AWS), Microsoft, and Google*", among others, generally own and operate the technology in their data centers, with access typically given through the Online platform.

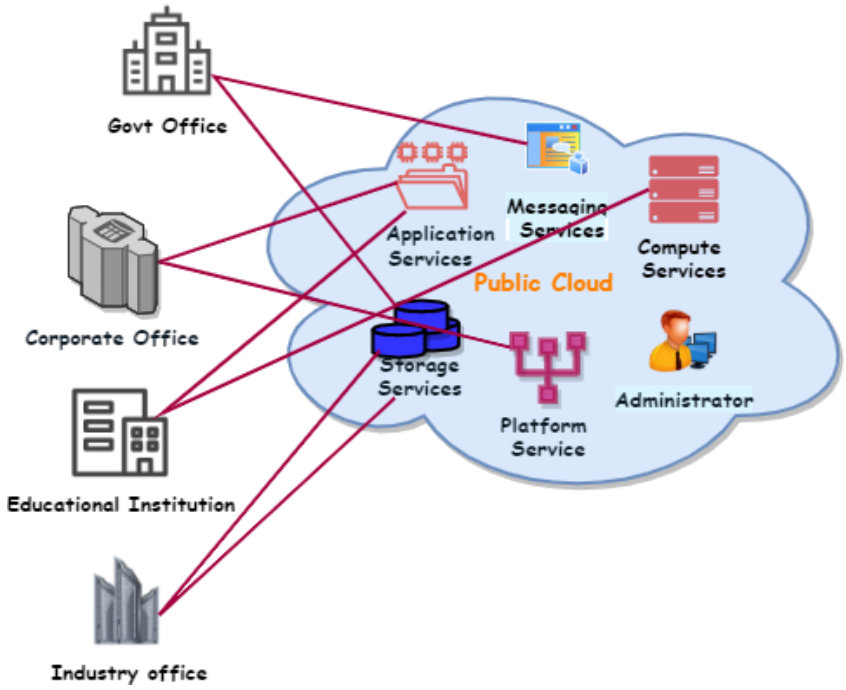

Figure 1.4 Public Cloud

CSP provide services in variety of sizes for billing purposes, which may be billed on a monthly, quarterly, annual, or leased basis. Primary providers such as Amazon Web Services (AWS) provide direct connect services known as AWS Direct Connect, while Microsoft's Azure provides a service known as "Azure Express Route."

1.5.2 Private Cloud

This cloud storage is operated mainly for security purpose when a userdecides that his or her data should not be available to the public. It is mainly operated by a single organization where the hosting activity takes place either internally or externally. A great deal of feasibility study should be done, when a company decides to create a private cloud, it demands the organization to re-evaluate current resources choices. When a private cloud was set up, it can improve the business turn over in term of millions or billions based the annual turnover of that organization. However, a company should address all sorts of security vulnerabilities before transferring all kinds of data (sensitive data like account number, medical records, password kind of things, etc.) to the private cloud. Self-styled data center is capital intensive but it as significant cloud-based in allocating physical space, hardware and environmentalcontrol.

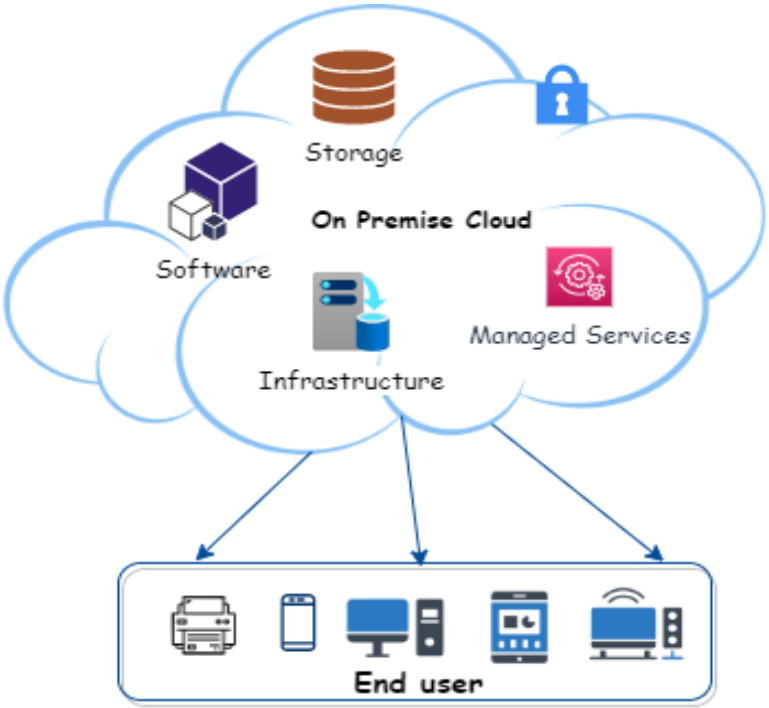

Figure 1.5 Private Cloud

Despite the fact customers are more drawn in towards the private, people see it as having a complex character at whatever point benefits must be reactivated periodically, resulting in massive additional overconsumption. Customers provided input since it was designed as a desktop framework for customers who needed to buy, manufacture, and maintain them on a regular basis. Private cloud is turning into a nature of talk because of the economy and captivating idea.

The engineering model of private cloud has appeared in Figure 1.5. On-premise private cloud construction costs a lot of money. Expenditure and hardware upgrade costs are included in the operational costs. When using an outsourced private cloud, the operating costs will be based on the number of resources used, which might alter at the service provider's discretion.

1.5.3 Hybrid Cloud

Hybrid apps, like inheritance, are mixture of double or tribble dissimilar clouds (private, communal, or public) that exist as independent entities then linked to offer users the benefits of several deployment methods. Figure 1.6 illustrates how a hybrid cloud may be used to put other clouds in a sequential way while also providing various characteristics of all clouds in a single set of objects. Since a hybrid cloud advantage transcends confinement and provider limitations, it cannot be easily integrated into a private, open, or public cloud benefit. It makes sense to extend the limit or capacity of a cloud benefit by combining, combining, or customizing it with another cloud advantage. A hybrid cloud may create a series of different clouds. For example, a company may keep sensitive customer data in a cloud-based private application to safeguard the privacy of its consumers. Nonetheless, the ability to connect to a business knowledge application hosted in an open cloud is a significant economic benefit.

Hybrid cloud environment may enhance an organization's capacity to provide a unique business service by expanding the number of publicly available public cloud services accessible from the outside world. It relies on several variables, including data security and regulatory requirements, the degree of data management needed, and the applications a business employs, whether or not hybrid cloud computing is used for its operations.

Another kind of hybrid cloud is when companies utilize public cloud when there is a sudden spike in demand and private cloud when more security is required. This feature allows hybrid clouds to use cloud bursting to achieve cloud balancing. It is a new application deployment method in which an application operates in a single cloud or data center for the most part, but when computing demand increases, the programme "bursts" out to a public cloud. In this approach, the application is installed in a private cloud or data center and then bursts onto the public cloud when more computing resources are required.

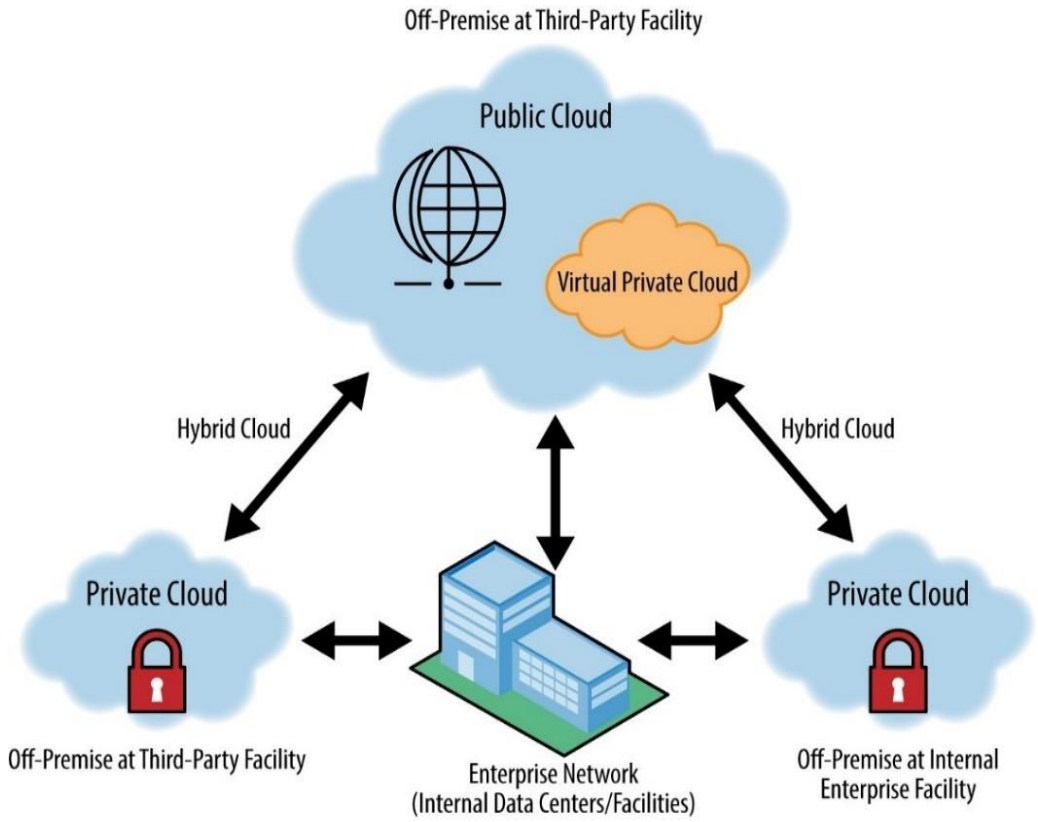

Figure 1.6 Hybrid Cloud

1.5.4 Community Cloud

This form of cloud infrastructure is offered primarily for users with similar concerns like purpose, policy, security needs, and compliance concerns. It owned, controlled, and managed by the society community, a third-party supplier, or their combinations. This could reside on or off-premise.

In that case, a community cloud can be defined as an infrastructure shared between those organizations, regardless of whether the infrastructure is overseen or facilitated internally or externally. In many cases, community clouds are used by businesses and organizations that collaborate on joint projects, apps, or research and require a centralized cloud computing infrastructure to develop collaborative projects, administer such projects, and execute such projects regardless of the solution provider.

The Department of Defense and many intelligence organizations, for example, have undertaken data center modernization projects utilizing a community cloud. This allows them to exchange data easily with other agencies through the community cloud while maintaining control and security. The costs are distributed across a few customers; thus, only a fraction of this cloud's cost-saving potential is shown in Figure1.7.

Figure 1.7 Community Cloud

1.6 CLOUD COMPUTING CHARACTERISTICS

Self-service that is available on demand:

Cloud resources may be supplied automatically without the need for involvement from the cloud provider, which is referred to as automated provisioning.

Broad network access:

Cloud storage is accessible via a standard method that encourages the performance of a broad area of client platforms such as mobile phones, workstations and laptop computers, as well as tablets and smartphones.

Reduced Costs:

Cloud computing may save you money by managing and maintaining your IT infrastructure. Utilizing the facilities of a CSP somewhat of purchasing more expensive systems and equipment for your firm may result in cost savings for your organization in some situations.

Resource Pooling:

Cloud computing's multi-tenancy features allow numerous users to share the same physical hardware. Virtual resources, which run on top of real resources, are given to users from different classes. Even though the customer does not have control over the bulk of assets, the customer could select a place that receives a greater degree of attention (e.g., nation, state or datacenter). For example, there are assets for storing things or preparing them. There are also assets for memory and system transmission capacity.

Rapid Elasticity:

Resource provisioning may be carried out fast and elastically. When needed, cloud resources may be instantly increased or decreased. Vertical and horizontal scaling options make the process easier by allowing the user to define parameters for scaling. According to application-specific data such as transaction per, CPU clocks per cycle, several simultaneous users, and request latency, users can scale their applications up or down as needed.

Improved performance:

Because resources accessible to applications may be scaled up or down based on dynamic application demands, provisioned resources enable enhanced performance.

Reliability:

Cloud-based application offers a better level of consistency since the cloud service maintains the underlying IT infrastructure. To ensure that cloud resources are reliable and accessible, service level agreements (SLAs) are used by cloud service providers. As a result, most cloud providers offer 99.99% uptime for their cloud resources, which might be difficult to accomplish with in-house IT.

Agility:

By using Cloud Agility, they can spend more time on other concerns such as security, monitoring and analysis and less time on providing and managing the resources they need. It enhances users' capacity to re-provision technological and infrastructural resources.

Measured service:

The main concept of cloud storage is pay for use. Cloud provider monitors the usage of cloud resources periodically and bills for the used resources. It provides transparency between customer and cloud provider.

Generally, it charges per hour or per month of resource usage so that subscription is never a big problem in cloud environment. Here, the customer need not pay in advance. Once the resources are assigned for a particular time period, then they have to pay for that period only.

1.7 PUBLIC CLOUD STORAGE

Public cloud storage enables organizations and individual users to easily lease storage space from a third party for the purpose of storing their digital data. The primary goal of public cloud storage is to allow individuals and businesses alike to store, edit, and handle data. This form of storage resides on a remote cloud service which is available via the internet via a premium service utility billing system in which users pay only for the storage space used.

A data provider provides decentralized cloud storage that publicly hosts, maintains and supplies the storage facilities to multiple customers. The phrase "public cloud computing facility" may also apply to storage as a service, utility storage, or online storage [18].

Popular public cloud storage capabilities include:

- ✓ Uncomplicated to make set up, self- conscience capacity
- ✓ Quite automated administration with rich APIs.
- ✓ Scaling of complex capability and efficiency
- ✓ Expandable mechanisms like links to disc, object and block.
- ✓ Either on-demand or monthly subscription price

1.7.1 Security Considerations for Public Cloud Workflows

Below are some of the most important factors for successfully protecting data and applications in the public cloud against a diverse range of constantly developing security risks that are frequently similar to those encountered in a conventional, on-premises data center environment.

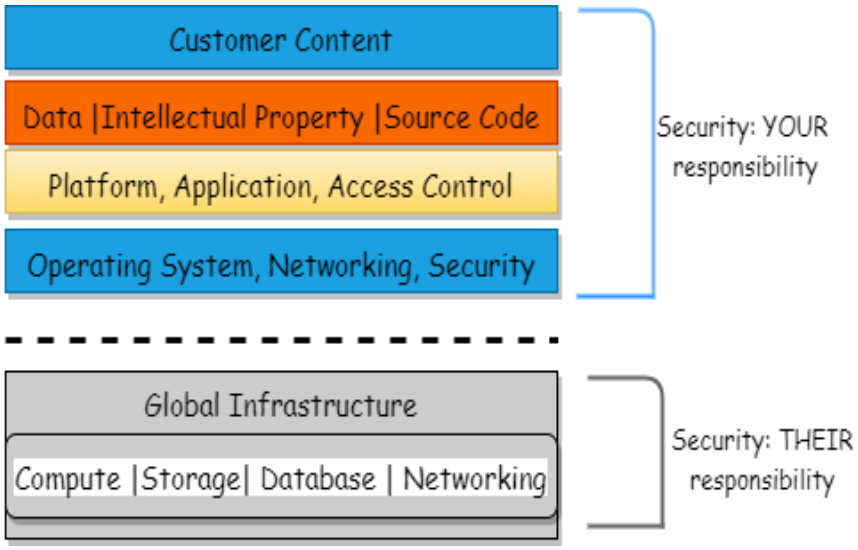

Figure1.8 Public cloud pooled accountability model

a. Endorse the model of pooled security

Public cloud companies, such as "*Amazon Web Services (AWS) and Microsoft Azure*", clarify that security is a pooled accountability. In this approach, the platform worker is responsible for guaranteeing that the platform is constantly ready, accessible, and modern, among other requirements.

Most respondents think that the cloud provider's worldwide data center set-up is extra secure than their individual data center architecture. But what has overlooked the reality that you, the client, are ultimately answerable for the security of your apps and data hosted in a public cloud environment. Workload security in a public cloud is no different from workload security on-premises, as illustrated in Figure 1.8. You have complete control over the security measures you choose to employ, and you must make efforts to protect your material, whether it be consumer information or clever stuff.

b. Early engagement through business sets and DevOps is essential

Multiple public cloud initiatives led via business organizations, such since DevOps, are tasked with rapidly launching new products or functional prototypes in response to market demands. In response to two factors, the general availability and adaptability of new reinforcement methods and the security organization often help with deployment. In an ideal world, security and DevOps would collaborate to recognize the breadth of public cloud schemes and guarantee the design of application deployments satisfies business development requirements while also minimizing the risk associated with security.

c. Prepare yourself for any possible exposure

A common term for public cloud use is "shadow IT," which refers to the simplicity of setting up a cloud account. It is possible for employees working in the "best interests of the business" to bring security vulnerabilities into the environment if the environment is not configured appropriately. It is essential to identify who uses the public cloud in your organization and ensure that the domain has been properly configured and set up.

- Lock down Secure Shell: Although secure shell is the ideal technique for securely controlling cloud services, it is frequently vulnerable in AWS and Azure settings.
- The encryption key and certificate inventories are often misunderstood by enterprises, allowing hackers to exploit them. A cyberthief with SSH access may easily conduct malicious network assaults from an organization's public cloud.

- Ensure Proper Configuration: Users should be aware that all outgoing ports on cloud platforms are left open by default, putting sensitive data at risk of exposure.
- Enforce Two-Factor Authorization: According to Verizon's most recent Internet Security Threat Report, 81 percent of hacking-related incidents used hacked or insecure passwords. Two-factor authentication is utilized to lessen the danger of identity theft.

d. Understand the Attacker

Attackers use automation to locate possible targets in minutes rather than hours. Then they seek for flaws, such as verifying default passwords and testing about misconfigurations, among other things.

e. Evaluate your security options

A variety of security options are available when transferring to the public cloud, most of which are equivalent to those available when using a conventional network.

Security for Native Public Clouds:

Security groups and web application firewalls are two types of cloud security services. They reduce the attack surface while introducing security vulnerabilities. You will not be able to identify or effectively manage the specific application granted access to your computer, nor will you be able to block it from accessing your computer's address bar.

Point Products:

Using a host-based point product is a common way of securing the public cloud. Domestic security combined with an IDS or IPS is what promotes this approach's popularity.

Security Do-It-Yourself:

Some companies seek to secure public cloud workloads utilizing scripting and visibility technologies. There are several possible disadvantages, including a lack of finances, a lack of expertise with security installation and operations, and inadequate support in a security issue.

In-Line Virtualized Equipment:

A virtualized in-line appliance, such as a virtualized next-generation firewall, serves as a basis for gaining insight into all traffic in your cloud deployment. Organizations may improve security for apps and data in the public cloud using application and content-based identification technologies.

f. Adopt a cloud-centric perspective

Comparatively to conventional IT infrastructure, the public cloud allows for a more rapid and flexible response to business concerns. To get the most out of the cloud, it suggests modifying data center principles to your needs while leaving conventional design alone. This provides high availability and scalability for organizations.

1.8 BENEFITS OF PUBLIC CLOUD STORAGE

For IT professionals, public cloud storage offers a wide range of benefits and applications.

- ✓ Public cloud storage can easily be deployed via a cloud-managed web portal or a service offered, for example the AWS Marketplace. A storage container requires no considerable technical knowledge, because the cloud provider manages environmental repair and monitoring.

- ✓ Storage space may be increased or decreased in response to changing needs. Furthermore, the performance limitations for the majority of workloads are sufficient.

- ✓ Cloud computing is accessible almost anywhere since the Internet is the gateway to the storage environment, which those may access via a search engine. In general, service providers provide services in several geographical locations, allowing customers to choose the closest to their business or that meets specific geographical or regulatory requirements. In addition, most cloud vendors have various storages to satisfy the needs of most applications, including file servers, object storage, and block storage.

- ✓ Flexibility is a prime asset for any cloud provider, the ability to launch the service easily. Licensing and execution will also take less than an hour, much quicker than hardware, or often more quickly than a fare for corporate IT capital.

- ✓ The majority of cloud providers offer scalable standards of service that enable end-users to choose the appropriate storage for their needs. Performance thresholds enable consumers to select, pay, and even modify amounts to meet changing performance requirements. Moreover, when companies leverage more cloud resources, being close to their files, they deliver efficiency gains over the management of data on the locations

- ✓ Whilst the long-term economic benefits of cloud storage can be discussed, few disagree about the economic benefits of obtaining cloud storage for transient purposes such as explosive workloads, cyclical or seasonal tasks, or merely backup and archive applications. With cloud applications being a higher priority, it would be much more advantageous to store and manage data close to applications.

1.9 SECURITY CHALLENGES IN PUBLIC CLOUD

Having remote teams working together from all over the globe means that companies no longer need a single physical location to store employees or data. Employees may access critical data from anywhere and anytime using public cloud systems like Amazon Web Server (AWS), Azure, and Google Compute engine. Access to the cloud may be adjusted up or down based on use to suit current work-from-home needs. With increased dependence on remote work in the foreseeable future, businesses may expand their cloud capabilities while operating in the normal course of business.

In 2020, Gartner predicted that the global public cloud services market would expand by 17 per cent, reaching $266.4 billion, increasing $227.8 billion in 2019 and $227.8 billion in 2019. As cloud computing becomes more widely used, it's critical to understand the difficulties businesses confront while using it. The Cloud Security Alliance has released the following list of key cloud issues [18][19]:

a. Absence of the architectural and strategic cloud security

Organizations all around the world are moving parts of their information systems to public clouds. During this period of change, a significant issue is the development of a good security design that can resist cyberattacks and keep the organization safe.

Regrettably, many businesses are still baffled by how this procedure is carried out. Because many companies believe that cloud service is just a matter of "lifting and shifting," or simply transferring their current IT stack and consisting mainly to a cloud system, their data is vulnerable to various dangers. Uncertainty about the shared security obligation paradigm is another element that contributes to this problem. [18].

b. Breach of Data

A data breach may have a variety of consequences, which include the following:

a. There are implications for consumer or partner confidence and loyalty.
b. Competitors were gaining access to intellectual property (IP), which may affect the launching of a product.
c. Regulatory consequences that may result in a financial loss.
d. An adverse brand effect may result in a reduction in market value owing to the factors previously mentioned.
e. Liabilities arising under the law and under contracts
f. Configuration errors and insufficient change control

It's one of the usually encountered cloud problems. In 2017, a misconfigured Amazon Web (AWS), Simplified System Storage (S3) online storage container revealed sensitive and confidential information about 123 billion American homes. The data set belongs to Experian, a consumer credit agency, which sold the information to Alteryx, an internet marketing and data analytics firm. Such occurrences have the potential to be catastrophic.

c. Inadequate management of identity, credentials, access, and keys

Cloud technology brings several modifications to conventional corporate system administration methods, particularly in Identity and Access Management (IAM) control. These don't need to be brand-new concerns. Instead, these are more important problems when working with the cloud since cloud computing dramatically affects authentication, password, and access management. Service providers and cloud customers are needed to handle IAM in public and private cloud environments without sacrificing security.

d. A potential insider threats

According to the Netwrix 2018 Cloud Security Report, insiders are responsible for 58 per cent of all security breaches in organizations. The majority of security issues are the result of insider carelessness. Ponemon Institute's 2018 Cost of Insider Attacks study found that 64 per cent of observed insider events were caused by team members or contractors' negligence, while criminal insiders were responsible for 23 per cent and credential theft was the root cause 13% of reported insider incidents. For instance, misconfigured cloud servers, employees who store sensitive corporate data on their devices and systems, or insiders who fall prey to phishing emails that lead to damaging attacks on company assets are just a few examples.

e. Harming an Accounts

In account hijacking, malevolent intruders acquire connection to and utilize credentials that are extremely privileged or confidential in order to commit fraud. When it comes to cloud computing settings, cloud service accounts or subscriptions are the accounts that pose the most danger. Phishing attempts, the manipulation of cloud-based services, and the use of data theft are all ways in which these accounts may be compromised.

f. Insecure User Interfaces and Application Programming Interfaces

It is possible for users to connect with and control cloud computing services via various software-user and APIs. General cloud security and availability depend on these APIs' safety for the cloud service provider's cloud provider.

There are several interfaces designed to guard against both accidental and deliberate attempts to circumvent the security policy. APIs that aren't well-designed may lead to misuse or, worse, a compromise of personal information. Security breaches have occurred as a consequence of APIs that were either misconfigured or hijacked. Organizations must understand security concerns for creating and providing these web interfaces [17].

1.10 CRYPTOGRAPHIC TECHNIQUES IN CLOUD COMPUTING

1.10.1 Need for cloud-based cryptography

The cryptographic cloud algorithms are used to encrypt data that are used or saved in the Cloud. It enables users easily and securely access pooled Cloud services since all data owned by cloud providers is encrypted. Uninterrupted cloud cryptography retains sensitive records. A variety of approaches are used to apply encryption to Cloud records. It's also possible to encrypt information earlier send to the cloud. It is useful since only team members with access to the decryption keys can decrypt the data before they leave the company or entity are able to decrypt the data. Other cloud storage providers will encrypt data before it arrives; ensuring that all information they collect and send is encrypted by design [20].

Although some cloud services have encryption as a standard feature, others encourage users to “bring their own” encryption. Customers must hold the control keys to keep their data encrypted, even if the encryption process arises in the cloud provider's environment. Cryptography in the cloud requires sensitive data to be protected in the absence of the business IT world. Cloud cryptography uses encryption methods to protect the cloud data. It allows customers to use public cloud resources conveniently and safely because all data hosting cloud providers are encrypted. Cryptography is the art or science of safe communication by translating the data into ways that cannot be interpreted. Cryptography nowadays is believed to be a mixture of 3 algorithms such that Symmetric key encryption, public key encryption, and Hashing algorithms [20] [21].

The plain text converted into ciphertext may be used in replacement techniques, in which a plain text feature, number, or symbol may be substituted by a character, and transpositions techniques used to encrypt plain text characters by certain permutations and combinations, different symmetric algorithm available, such as DES, triple DES, AES, Blowfish and IDEA.

These algorithms operate on multiple input blocks and input size keys. Two keys are used by asymmetric key algorithms, one to encrypt and another to decrypt. Different asymmetries are used, such as RSA and Diffie-Hellman.

1.10.2 Cryptographic Cloud Storage

Cloud storage is vital for the security of our private data, and safe storage must be accomplished in cloud computing if any unauthorized access is possible. Thus, we follow protected storage cryptographic methods, which are secured until the data is submitted into the cloud by the data owner. Cryptographic Cloud Storage Strength mostly depends on Confidentiality, Competent and Integrity.

Confidentiality: Cloud Storage Cryptography Provides confidentiality and is the key feature and encrypted by sophisticated encryption methods to preserve privacy [19].

Integrity: Cloud Storage maintains data integrity and thereby prohibits unauthorized entities from manipulating the data.

Competent: The time required to retrieve data is comparable to a public cloud-based cloud platform.

As shown above, figure 1.9 depicts a cryptographic cloud warehouse, and data owner uses encryption techniques to prevent unauthorized access to confidential data. The data owner can import encrypted data into the cloud system, and the approved user can decipher the data and upload the file.

An essential characteristic of a cryptographic storage provision is the security qualities indicated up are provided by solid cryptographic assurances rather than legal, physical, and access control procedures, as with traditional storage services.

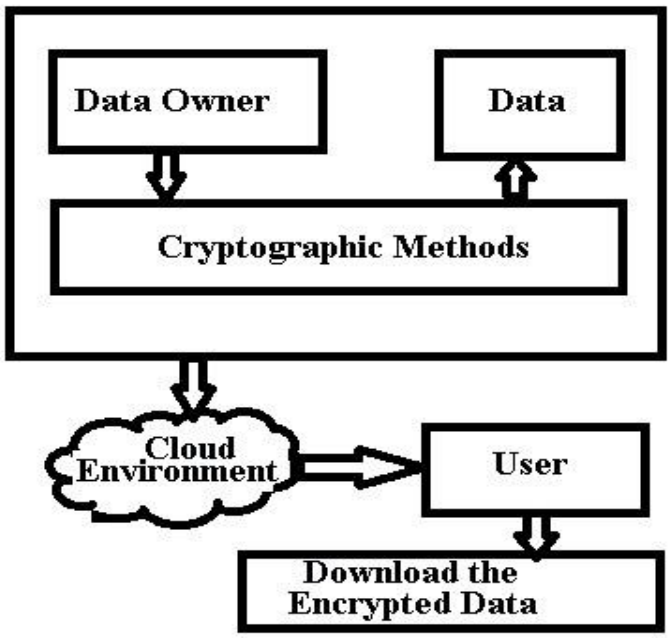

Figure 1.9 Cloud Strategy

1.10.3 Techniques (Algorithms) in Cryptography

Several current methods are used to enforce cloud storage protection. Below are some of the latest analysis encryption algorithms [22].

- *DES Algorithm*

This algorithm is a widely used and IBM laid it down in 1974, but various methods present-day show that this algorithm has not been achieved [23]. DES algorithms contain a 64-bit block cipher [24]and the 56-bit key used for 64-bit key is a used eight-bit rest.

In such a single block encryption, we encrypt a plain text data block using a combination of uncertainty and diffusion in order to make cipher block then it goes through 16 rounds and divides the 64bit data into 32bit.

The Feistel function is implemented until the data have been divided into 32 bits. F-function requires substitution, permutation, and combining of the key. The o/p function uses an XOR alternate data crossing to blend with another half of the data and the data crossing will be finished [25].

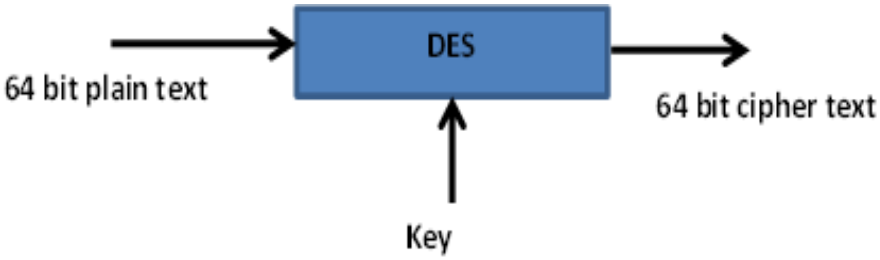

Figure 1.10 High Level Diagram of DES Encryption Algorithm

The downside of DES is that the DES key use key is very limited and its protection can easily break up, and the DES only operates quickly on hardware and slowly operating on software, until 16 rounds ciphertext is developed or data encryption is done, for reverse data decryption is performed [26].

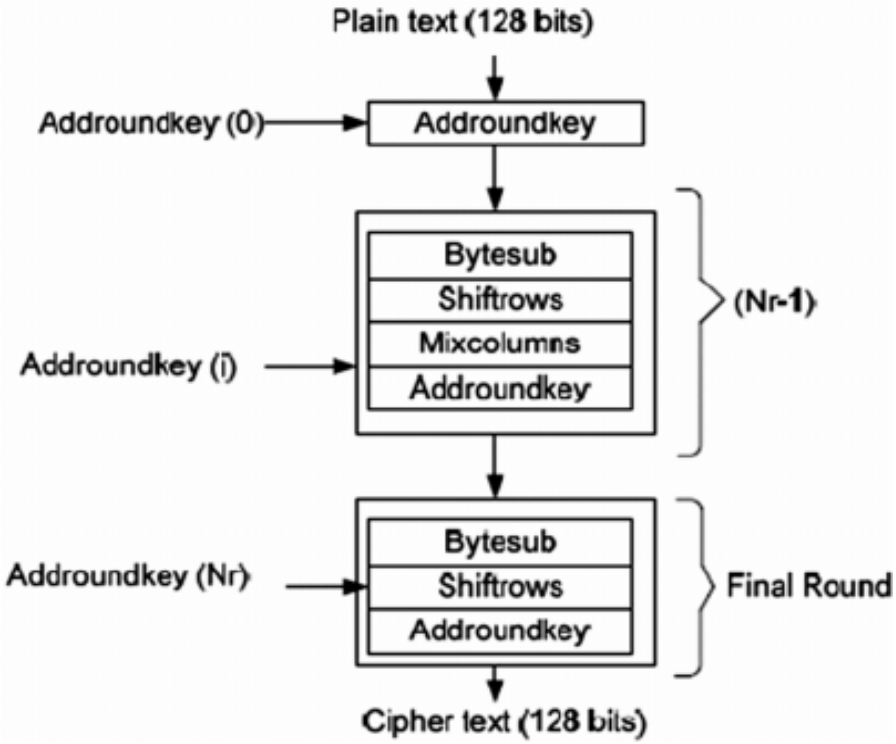

Figure 1.11 Encryption with AES Algorithm [6]

- *Advance Encryption Standard Algorithm (AES)*

Depending on the number of iterations used, this algorithm uses 128bit, 192bit or 256bit key. This means that a 128bit key will take 10 rounds, a 192bit key 12 rounds and a 256bit key will run 14 rounds. AES operates on a 4 X 4 grid and AES is a fast encryption algorithm that works on both hardware and software [27].

- *RSA Algorithm*

This method is built on an integer positive function. For decryption and decoding, RSA uses modular exponential. RSA is a fixed-key cryptography algorithm with a Public Key (PK) and a Private Key (PK). Each client has public key access to which messages are encrypted. Only private keys are decoded for messages which were encrypted using the public key. Figure 5 illustrates the operation. RSA uses 2 exponents such as *'d'* and '*e*', with '*e*' being the public and '*d*' being the private. Allow M be the plain text and C be the ciphertext, and then proceed to encoding [28].

1.11 PROBLEM STATEMENT

Customers may use cloud computing services that include large-scale processing, data storage, virtualization, excellent portability, high dependability, and low-cost service. The storage of data in cloud is more sensitive to users as it is stored in the third-party storage and it is one of the major problems identified. Firstly, it is necessary to safe guard the data whenever the data is uploaded to data center to ensuredata is not tampered on the way to cloud storage. Second, anytime a hacking incident occurs, the information saved in the cloud is freely available to the public without any security.

Thirdly, even though a security mechanism is employed in cloud storage, accessing and retrieval of data from the storage raises another issue of efficiency and availability. Improved security and quick cloud data retrieval without sacrificing security have long been an urgent need. In this thesis an efficient improved scheme has been proposed to solve the aforementioned problem for the data stored in public cloud storage as well as during data transit.

1.12 ORGANIZATION OF THE THESIS

Chapter 1 of the thesis provides the required introductory concepts of Cloud Computing. This chapter discusses the various services provided by cloud computing, different deployment models available in cloud computing, public cloud storage, safety challenges in public cloud and cryptographic techniques in cloud computing.

In Chapter 2, many writers in the subject address the numerous schemes and approaches they've devised to assist their problem-solving, research goals, and methodology.

Chapter 3 addresses the risks and challenges that an organization experiences when using cloud-based applications and the differences between conventional data storage and cloud data storage and cloud storage concerns.

Chapter 4 presents the proposed MBO-ABE method for public cloud storage and includes experimental findings demonstrating the effectiveness of the proposed technique for secure public cloud storage.

Chapter 5 explains the PCE (Parallel Chunk Encryption) scheme that uses the forward encipher approach to protect public cloud storage and the results and discussion obtained from the scheme.

Chapter 6 summarizes the thesis's research objectives and makes recommendations for further research.

CHAPTER 2

REVIEW AND ANALYSIS

As cloud computing has grown in popularity, the number of individuals worried about security has increased. The data security of cloud storage is a difficult challenge for researchers to solve. Thus, while developing security algorithms, it is more critical to focus on the time required for encrypt and decrypt, the method used to create unique cypher text from plaintext, and the number of layers utilized to create the cyphertext from the plaintext. Confidentiality, Integrity, and Availability are the criteria for determining data security.

It is possible to maintain data confidentiality by restricting access to the data to only authorized individuals. If you want to keep your information safe from unwanted access, you need either encrypt or disguise the information. There are many worldwide conferences that are solely focused on cloud security and there are many international publications dedicated to public cloud storage security research.

Several survey studies are featured in this area, which are the best we can tell you about them based on our information. This chapter provides an overview of various current methods and schemes that rely on public cloud data storage security, as well as an explanation of their benefits and challenges.

2.1 REVIEWS OF EXISTING SECURITY METHOD AND SCHEMES IN CLOUD STORAGE ENVIRONMENT

J. S. Resende and colleagues.[29] was shown that a new design might improve data confidentiality and availability across tiny footprint devices, such as Internet of Things systems, compared to the existing state-of-the-art architecture. It uses erasure coding and cryptographic methods across various storage providers to offer a dependable and privacy-preserving solution for users.

ARGUS offloads computation from the client to accommodate resource-constrained devices, such as mobile devices. Although they did not account for optimization problems, the author said that the system performs better in terms of upload time when compared to Google Drive.

H. Graupner, et al. [30] developed Asymmetric Convergent Encryption (ACE), a flexible system combining the advantages from context-sensitive partitioning, concurrent and distant updating protocols to reduce the uncertainty of breaches on data security and maximize storage utilization. Furthermore, because of the protection provided by the Asymmetric Convergent Encryption proof-of-data-ownership method, their approach prohibits unauthorized access to sensitive data (ACE). It is analogous to others with the performance evaluation. The actual parameter used: min. partition size = 1 KB, max. Size of the partition = 16KB and size of the Rabin window = 192 B. It indicates the deductibility of public data collection. Performance is always a major component of discussion when it comes to usable security. The primary drawback of the paper is not user administration, key management and access management.

S. More et al.[31] propose a method for protecting cloud data. They utilized AES for data secrecy and TPA for data auditing in their process. They generated the message digest using the SHA-2 algorithm. They make no mention of the AES(128,192,256)version used. Additionally, they did not specify which version of SHA-2(224,256,512) was used. The author did not determine how data are divided and encrypted; we cannot conclude that their method is safe since all versions of AES and SHA are secure. Y. Ren et al. [32] proposed MV-PDP system is a sort of data possession mechanism. When a client signs data blocks, the data blocks may be confirmed by a private verifier, and the same data blocks can be signed and reviewed by both parties with relative ease. To construct their system, they use an ECC-based homomorphic authenticator, resulting in reduced computation and communication costs since the bilinear operation is unnecessary.

X. Li et al.[33] Investigated the public audit scheme of Fan et al. and gave extensive demonstrations to demonstrate that the technique was not secure. They showed that the malevolent cloud verifies the auditor by creating legitimate evidence, even though the user data is not stored. This method is thus not safe. If the consumer wishes to a save file to the cloud $\{m_1,..., m_n\}$, it will calculate the file tag {M' Ɵ, tag } then he will send it to the cloud once the file and tag have been received just a portion of this file is deposited on the cloud and others are deleted. The author has shown crucial analysis to prove that the spiteful cloud may still give the auditor check if the user data has been removed or changed.

Wang, C et al.[34] have suggested a method to enable public auditing while maintaining privacy; in their approach, HLA and BLS signatures and MHT are utilized. The Merkle hash tree is used to support data in their method dynamically. Additionally, they have preserved their integrity. Confidentiality is not maintained in their process, and intrusive auditing is encouraged.

To protect public cloud storage services, Nelmiawati et al. [35] created an app called dCloud, based on Java. dCloud is a combination of Rabin IDA and SSA Shamir utilized to deliver confidentiality, integrity and access to the public cloud storage providers as a core secret share algorithm on dCloud. In the dropbox plugin, dCloud is integrated. The main downside is more plugin need for expanding the support of dCloud to another provider since data saved in public cloud storage is less available. Optimization is needed, especially when dCloud is utilized on mobile applications because it has limited CPU and memory resources. C. C. Erway, et al. [36] presented an effective data possession dynamics system (DPDP I). The audits in this system, however, do not safeguard privacy.

G. Amalarethinam, and colleagues [37] proposed a method known as CBO, which stands for confidentiality enabled obfuscation. People and organizations both may benefit from cloud storage services since they are both cost-effective and convenient. According to the suggested method, data is disguised before being uploaded to a cloud storage service like Amazon S3. According to an experimental result, the CBO method improves data security while simultaneously lowering the cost of data storage. Sidhu, A et al. [38] suggested enhancing the security of the CC structure via hybrid encryption, which uses double encryption methods, one for plaintext and another one for previously encrypted data. The system is identical straightforward in implementation and may do in a short period. The practicality is doubtful from a security standpoint since significant encryption techniques are mentioned without further care being taken to protect the encryption keys.

Y. Xue, et al. [39] The CP-ABE system was established and promised to provide sophisticated, elastic and safe access power for outsourced information in public cloud. The primary downside is that a single attribute authority must undertake the time expensive verification of user validity and secret key distribution.

This means that the execution of the CP-ABE programme in a large club store system results in a one-point performance bottleneck. For a lengthy time, users might stay at the queue to get their secret keys, resulting in low system efficiency. Although multi-authority access control methods have been presented, the disadvantages of single-point bottlenecks and low efficacy cannot yet be solved as every single authority still administers a disjoint attribute separately.

In order to avoid the unwanted path to cloud dataset in a public cloud, L. Zhou, V et al.[40] presented a rolled encryption method merging cryptography technique with roles-based entrance power. The architecture enables organizations to safely store data on a public cloud while retaining the confidential structural data in a privately-owned cloud. They have also created a secure cloud architecture for the storage systems and own proven that it has numerous better features, such as constant chip text and decryption key. Test observation shown both encrypt and decrying calculations on the customer side are cost-effective, and numerous cloud-related processors may decrease decryption time in the cloud. The system uses bilinear pairings with intensive calculations.

J. Yuan, et al.[41] The author presented a constant-cost method for simultaneously achieving safe public data integrity auditing and storage deduplication in this study and verified the scheme's efficiency and scalability through numerical analysis and experimental findings on Amazon EC2 Cloud. Additionally, the suggested polynomial-based authentication tag may be utilized independently for other related applications such as verified SQL search, encrypted keyword search etc. J. Liu, et al. [42] A redundancy-based, efficient and secure public cloud audit protocol based on 'POR, PDP, POW and SCS, POSD and PCAD' schemes, among other technologies, was suggested. The effectiveness and security of the SPAD scheme are shown via numerical computation and analysis of experimental data. Compared to existing PDP/POR/POW solutions, the SPAD scheme provides a more comprehensive, efficient, and secure functional capability. W. Shen, et al. [43] A public cloud auditing method with lightweight authenticator generation was proposed to minimize users' computing load. Developed a novel public cloud storage auditing architecture in which an AGC creates authenticators for users. In the proposed method, actual cloud data cannot be disclosed when authenticators are generated to the AGC.

In addition, the cloud may check if the authenticators produced by the AGC are accurate. Y. Zhang, et al.[44] Suggested an authorized public cloud identity audit system with a hierarchical construction, which is well used to generate private keys and authenticate identifying identities for more significant users and has a hierarchical PKG structure that can delete the PKG root – the PKG lower level gates. On this basis, a new cloud storage audit system was developed. The approved lowest-level PKGs may only represent users in their appropriate domains to validate the truthfulness of cloud data. Cloud data availability not mentioned.

To protect the confidentiality of numeric and non-numeric data, S. Arul Oli [45] proposed the "AO ARO EncObfus CT" method, which complies obfuscation and encryption to achieve this goal. Furthermore, the obfuscation of mathematical data alone organizes not provide enough security for the information that has been stored on a computer system. This article provided a technique for safeguarding both non-numerical and mathematical data at the same time in order to enhance overall security. The recommended approach also resulted in a reduction in service costs, data size, and processing time when data was uploaded into CS. As a consequence of this strategy, remedies to the security problems that presently exist in the current scenario have been developed and implemented.

C. Hahn, et al. [46] suggested a tamper-resistant commitment method for public cloud storage in this research. The presented technique may be used in conjunction with any ABE system that utilizes external decryption capabilities. They conducted security and performance studies to demonstrate that the suggested method is resistant to tampering while seldom reducing efficiency compared to existing techniques. X. Dong, Yu, Y. Luo et al. [47] established a system for cloud computing data sharing that is both privacy-preserving and safe by combining CP- Attribute-Based Encryption with the IBE methodology, described in detail below. A fine-grained data access control mechanism is provided, and backward secrecy, safety compared to user cooperation with the cloud, support for user adding, overturning, and attribute changes in the proposed approach. The use of computational overhead necessitating the use of matching methods has been identified as a drawback. X. Ding, et al. [48] presented a arbitrated *"Certificate-Less Public Key Encryption"* without coupling procedures, addressing critical escrow and revocation issues.

The method enabled immediate revocation and guaranteed data secrecy deposited in untrusted public cloud while adhering to the data owner's access control rules. This enhanced approach encrypts each data item just once, reducing the data owner's total overhead. The suggested system is not entirely immune to insider attacks.

T. S. Fun, et al. [49] Examined the security defense mechanisms of current public cloud service providers after reviewing password-based attack scenarios. However, current password-based methods are susceptible to password-based attack models owing to the predictable pattern of the user's chosen password. They recommended a Honey Encryption method that improves public cloud file storage security by increasing the difficulty of differentiating between accurate and false data. The author recommended that their work be expanded by combining HE with Honeywords to secure user authentication and login sessions.

C. Liu, et al.[50] Introduced a novel public audit method as MuR-DPA. The novel method included a unique validated data construction based on the MR-MHT. Because of this, it has a reduced connection latency while doing both updated confirmation and integrity verification on the cloud dataset. Despite all of these benefits, the size of the proof still relies on the size of the dataset.

R. Sugumar, et al. [51] A Symmetric Encryption Algorithm has been proposed to protect data stored in public cloud storage. SEA transforms source text into ASCII code, which is then used to handle the data throughout the encryption process. Encryption and decryption are proficient with the support of two symmetric keys. These keys are stored on the computers of the cloud handlers. Cloud storage should only be accessed by those to who the cloud service provider has granted permission. The suggested SEA thus assists cloud service providers and customers in maintaining security in a cloud environment; however, the disadvantage is that authorized individuals are not permitted to access public cloud data in this SEA.

Hadi, S et al. [52] presented a novel related-key that is invulnerable to various time-complexity attacks. The attack relies on a unique feature of the mix column operation. A. J vanyan and colleagues. [53] A Skycryptor was created to convert public cloud storage into privately secure environments without affecting the usefulness and convenience of such storage.

Skycryptor makes it possible to handle encrypted information more efficiently, which results in a more user-friendly experience for the end-user. Future work will include full-flow testing and benchmarking, which will be placed once the service is made publicly available. W. Wang, et al. [54] recommended a public auditing approach for Cloud Computing data storage security that protects user privacy while guaranteeing data integrity. They utilized the homomorphic authenticator and random masking methods to guarantee that TPA did not get any information about the data deposited on a cloud server. According to the results of the extensive research, the suggested methods are both provably safe and very efficient.

S. Cherillath Sukumaran et al. [55] suggested a DNA-based encryption method for securely storing information in the cloud, where data storage is a significant issue and security is a significant concern for SaaS customers. The method will improve security by increasing computational complexity via the use of biocomputing techniques in addition to cryptography. The user may validate the data without depending on a third party. The suggested DNA Cryptography is a new encryption approach for safe data storage in the cloud environment; the method is rudimentary, but utilizing DNA cryptography for the cloud has great potential given the significance of cloud storage in industries and daily life.

R. A. Id, N. Z. Id, et al. [56] proposed and analyzed a new technique called Tagging of Outsourced Data (TOD) that may be utilized in DIA to solve the problem of regularly verifying the integrity of data maintained by third parties without downloading the whole data set PCS. Additionally, the report included a thorough security analysis and a theoretical and experimental assessment of the method's overhead costs. The assessment findings are compared to those obtained using comparable tagging techniques. The study and comparison findings showed that, compared to comparable techniques, TOD is more efficient, especially for user endpoints, and offers greater capabilities, including enhanced data security.

X. Yu, et al. [57] developed and deployed the SEHadoop architecture to enhance compromise resistance on a public cloud. Using this architecture, you may increase the amount of isolation between Hadoop elements while still following the concept of minimum access privilege.

According to the findings of the experiments, improved isolation and least access rights prohibit attackers from leveraging agreed rules to compromise the remainder of Hadoop's component processes the trial results also showed that moving tasks to SEHADOOP is simple and has minimal effect on performance. K. Liang, et al. [58] Introduced the concept of DFA-based FPRE and an implementation strategy that complies with the new idea. Moreover, it demonstrated that the system, the first of its kind, was adaptively CCA secure in the standard model by including Lewko et al. encryption technique into the design. This study sparked the development of several intriguing open issues. One of them is transforming our DFA-based FPRE into a prime order bilinear group, which is a difficult problem.

N. Kaaniche, et al. [59] Determined to combine the increasing need for safe cloud storage services with the appealing features of ID-based encryption, resulting in a unique solution to the data outsourcing security problem. The solution is based on a particular use of IBC. The IBC–PKG function is first allocated to cloud storage customers. As a consequence, they may make their public components public while keeping their IBC private. Second, to encrypt data, a per data key generated from a data identifier is utilized. This work is demonstrated to enable data privacy and secrecy thanks to IBC characteristics since it uses an innovative ID-based client-side encryption method. O. Arki, el at. [60] The suggested framework is built on the "*multi-agent systems paradigm"* an expansion and encryption method to ensure data security. RSA method is used to authenticate the user authenticity via digital signature. Small-size files transferred among the data owner and cloud provider are secured using RSA to secure all communication. The integration of both AES and RSA algorithms are proposed encryption technique offers a better way to guarantee data secrecy while also increasing the speed of the encryption method.

D. Tiwari, et al. [61] The purpose of maintaining confidentiality both in the past and in the future, and encryption proxy system using ciphertext policy characteristics were proposed. This system also contained a fine-grained revocation mechanism. A multi-authority key center is used during a key-making process to alleviate constraints and key exchange concerns. By conducting a comprehensive performance and implementation analysis, the proposed system improves the operational effectiveness of storage, computation, and implementation cost.

H. Tian, et al.[62] Auditing information and block tags may be sent from a CSP to a TPA using the suggested approach, which reduces computational and announcement aloft. According to studies, a cloud auditing system effectively produced a secure auditing process while incurring much-reduced storage and communication costs than past methods. In addition, the system employs the BLS signature methodology from bilinear maps to perform many auditing tasks at once.

Y. Peng, et al. [63] Examined secure cloud storage, a sub-offering inside the IaaS (infrastructure as a service) cloud computing model developed utilizing cryptographic methods. Rather than paying too much attention to the specific structure of cloud storage, this paper focuses on the types of cryptographic techniques that are operated and how they are used in cloud storage architecture. The usage of additional cryptographic methods in cloud computing and the development of more secure cloud storage systems are expected to increase in the future. R. L. Contiu S., et al. [64] investigated and compared the performance of various cryptographic primitives often used to provide security and privacy in public cloud storage. The purpose of this experiment was to evaluate the costs and efficacy of several cryptographic primitives for protecting public cloud storage, not to create novel methods. They performed a series of tests on six distinct cryptographic techniques in order to determine their raw speed and performance in a natural cloud storage environment. The findings demonstrate that the optimal scheme for one scenario, such as a write-intensive task involving mainly tiny files, may not be optimal for another, such as a read-only workload involving big files.

Z. Xu, et al.[65] established that Yu et al 2016 method is susceptible to data recovery assaults. These attacks are effective because they enable an external attacker acting as a TPA to discover the contents of data blocks simply by gathering auditing information. To address this security vulnerability, we suggested an enhanced public auditing method that accommodates variable-sized file blocks. The security study established that the proposed ID-SEPA system is safe and capable of meeting cloud storage security criteria. The suggested scheme's thorough performance assessment showed that it achieves a better degree of security assurance while incurring a small increase in computing costs. As a result, the system is better suited for implementation in the actual world.

A. L, S, et al. [66] used the round key AES with Honey method to secure public cloud data storage. The absence of safe storage for the AES algorithm's private key in the previous system has effectively removed in the created system by storing the AES's private key after it has been encrypted using honey Encryption. The result is the provision of a fully secure AES Algorithm. As demonstrated in the comparative table, the addition of the honey method does not affect the AES algorithm's performance or cost. These approaches successfully address the brute force assault, the side-channel attack, and the difficulties in the key management area.

J. Lai, et al. [67] We developed a Ciphertext-Policy ABE system that supports policies as any monotonic tree access structure and is resistant to collusion attacks. An attacker may obtain multiple private keys. It would be fascinating to explore attribute-based encryption systems with varying degrees of repressibility in the future.

A. Irudayasamy, et al. [68] suggested a highly scalable parallel BUG method for large-scale data anonymization via Bottom-Up Generalization (BUG), and partitioning and anonymizing datasets in parallel is the first step. The second step merges and anonymizes the intermediate findings to create consistent k-anonymous data sets. For scalable Generalization calculations, the map-reduce method has been used creatively on the cloud to data anonymization. On real-world datasets, BUG outperforms all other approaches in terms of scalability. Protecting privacy in the cloud environment is a difficult research problem as bigger and larger datasets are utilized. Data anonymization techniques are thoroughly investigated. To maintain overall scalable privacy, heuristic the balanced scheduling methods are required.

P. Voros, et al. [69] described methods for preventing data breaches, the most prevalent online danger targeting personal details, outlined several network designs, and showed how an extra security layer might help improve the security of personal data stored in the public cloud. Because OpenWebCrypt is a client-side lightweight browser plugin for individual users, it acts as a prototype. CrypStore PI is a proxy-style encryption device that guarantees no unencrypted data leaves the trusted network and distributes encrypted data across several public cloud storage providers. Additionally, demonstrated the performance of different encryption methods on our specialized hardware.

Hong Zhong, et al [70]. Authors study look into fuzzy access control strategies for cloud storage systems. A new concept of secure decentralized CP-ABE approach for designing an access control system that conceals policy information was proposed. The access control technology ensures that data and access policies are kept private, and it uses a more flexible LSSS matrix access structure to achieve this goal. Also included is support for efficient user revocation for multi-authority CPABE, which reduces the communication and calculation costs associated with user revocation and ensured the security of the schemes and evaluates their performance. Yong Cheng, et al [71]. The author developed the first mechanism for revocation without the assistance of a third party. The author demonstrates how to include the efficient technique into a CP-ABE-based cryptographic access control system and then evaluates its security and reliability characteristics. Revocation occurs often, and the efficient revocation technique surpasses the complete process in terms of efficiency.

2.2 SUMMARY

The usage of public cloud storage services allows businesses and end users to simply lease storage capacity from a third party to store their digital data. Many companies fear the security and confidentiality of data deposited inside a public cloud service since everything in a public cloud environment is out of their control. The absence of direct control over security measures is one of the most significant disadvantages of this system. Data security and user privacy are of utmost importance in business settings, such as the healthcare industry. One major drawback of using a public cloud is the inability to manage security measures actively. The purpose of the research and the security issues related to public cloud storage are discussed in this chapter.

During this study, various aspects of security problems have been analyzed. Literature review reveals that most of the researchers have contributed their work related to data security, and it is encouraged to propose the new algorithms. Hence, the public data cloud storage environment needs optimized security schemes and cryptographic techniques to assure the security of public cloud storage.

CHAPTER 3

SECURITY RISK ON DATA STORAGE IN CLOUD BASED APPLICATION

This chapter polestar on security challenges and risk faced by different organization while storing data on cloud storage using application software and specifically discussed based on public cloud storage.

3.1 INTRODUCTION

A cloud storage system is essential in today's environment, replacing traditional storage devices. Because of the events of their technical or personal lives, people get to deal with thousands of megabytes of data every day [72]. All this information takes a lot of storage space and consistency in its availability around the clock across numerous devices widely used and linked by users to get their job done [72]. Cloud Computing, Internet-based growth, and broad information and communication technology usage are ushering in a new era. With the advancement of technology, processing power has become more economical and powerful. On the other hand, SaaS computing architecture is transforming data centres into enormous pools of computing resources. In recent years, clients have been able to sign up for slightly elevated services based on information and technology that is entirely stored in remote data centres due to increased network capacity and reliable yet flexible network connections.

However, despite its potential as an internet-based service platform, this new data storage paradigm in the "Cloud" introduces a slew of complicated design concerns that significantly impact the entire system's security and speed. One of the most severe issues about cloud file storage is the lack of data security authentication on platforms that are not trusted by the organisation storing the information. However, due to the expense involved and a few other variables such as the system model or the technology they use to operate, the actual storage space has a drawback. A modern, fast, and low-cost technology has been developed by many businesses to solve the challenges o-f storage and usability issues of data for users, widely known to the world as Cloud Computing.

Depending on the circumstances, it may be acceptable, or at the very least feasible, for an individual to store data on distant cloud servers. These include the following three critical states or situations that are specific concerns within the cloud computing operational context:

- The transmission of confidential, non-public data to a cloud server
- Transmitting information from the cloud server to the operating systems of the customer and
- Storage of non-public data from clients on cloud servers that are remote servers that buyers no longer own.

All cloud storage is severely vulnerable to a violation of security that makes analysis and investigation fundamental within the safety factors of cloud computing practice users connect their data files to the cloud. They leave the data in a position where they are out of their power. Typical cloud threats include misuse of information, malicious insiders, unstable boundaries and APIs problems with common technology, information loss or leak, capture of accounts or services, and an unknown profile danger [73]. Organizations providing cloud providers provide applications, principles, or support as a service [73]. The provider must ensure that data and applications are secured against security problems faced by its clients. The client must verify that the supplier has implemented security measures to safeguard their personal information. Social networks are internet tools that allow users to connect with their friends and share interests, and they are getting more popular.

Users upload material to the programme to keep their connections up to date and share personal news, successes, hobbies, and other information. Standard social networks, such as Facebook and Twitter, have hundreds of millions or possibly billions of members spread over the globe, all of whom are exchanging data linked together. There is always a trade-off between the expense of data storage and the latency of the system. A viable approach would be to keep the data associated with each user in every accessible data centre. The expenditure would become unfeasible and uneconomic over time as the quantity of users increases. Cloud Data centres are the superior option for lowering the costs associated with data centre establishment and maintenance than traditional data centres.

Geographically dispersed cloud services with nearly limitless capacities are well suited for storing enormous amounts of data from social networks in various geographical regions on a big scale.

3.2 TRADITIONAL DATA STORAGE VS CLOUD DATA STORAGE

Conventional data warehouses are made up of several hardware components linked to a network via the use of a remote server, such as a desktop computer. Most servers are installed on-premises, and they offer access to the company's stored data and applications to any workers who have access to the hardware. Companies that use this IT strategy must purchase more hardware and make changes to scale their data storage and services to serve many clients. It is also necessary to have obligatory software updates for conventional IT infrastructure since hardware failures may cause unreliable systems to collapse. An in-house IT division is responsible for developing and managing hardware for many companies that operate IT data centres. Many businesses with IT data centres need an in-house IT staff to build and maintain the gear.

Among the most secure information hosting options is an essential IT architecture that enables you to manage your business's apps and data processing entirely on a local server. The customized, dedicated platform is ideal for companies that need to operate a variety of app kinds. As a virtual storage system, Cloud computing is much more abstract than the traditional method of accessing data through hardware resources. All server applications and systems are moved to the cloud, which is located off-site. Instead of investing money on purchasing physical servers for your company, you may lease digital storage space from the cloud-based services based on a much more cost-effective wage, saving money in the long run. Many separate servers host an authentic virtual environment in the process, known as a distributed virtual environment. Extrinsic data storage and delivery methods like cloud computing are less secure than on-premises hosting, which may have an impact. The stored information and applications can be located and used in the cloud by anyone with access to the server, anywhere a web link is available. When transitioning to the cloud, selecting a fully transparent provider in its hosting of cloud platforms and ensuring optimal security rules are in place is essential.

By using strategies such as firewalls and virtualization, the Cloud Provider vowed to guarantee data protection over client stored data. Because of their weaknesses across the network, these methods would not provide comprehensive data security because CSP has complete control over cloud apps, infrastructure, and customer information. The working model of cloud data storage as shown in figure 3.1.

Cloud Security	**Traditional IT Security**
Third party data centre	In-House data warehouse
Infrastructure investments are insufficiently prepared	High in readiness costs
Rapidly scalable	Unrushed scalable
Protective resource utilization	Low efficient
Costs are determined by the amount of data stored	Data preservation is becoming more expensive

Table 3.1 Traditional Security Vs Cloud Security

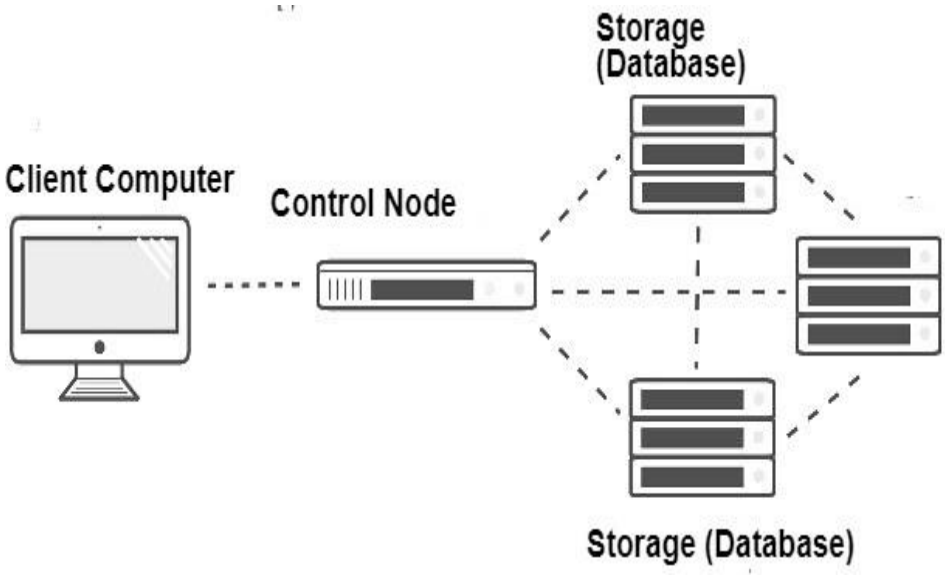

Figure 3.1 Working of Cloud Data storage

3.3 DIFFERENT CLOUD COMPUTING PLATFORM FACING SECURITY THREATS

3.3.1 Education Cloud

Currently, online education is widely utilized in the educational sector. The sharing of resources and the incorporation of materials are significant concerns, especially with the increasing use of the education cloud. It is becoming increasingly important to consider security issues about the education cloud, such as data loss. Because of the need for large-scale tutoring administration and education, the academic cloud has the features of high connectivity and huge dependability on a large scale, which makes it ideal for education. [74]. When protecting their data from possible breaches and data loss, cloud service providers rely on fundamental data security methods such as encryption and access control [72].

As a result, we found a risk of data leak, data fall, and security assaults on an academic cloud infrastructure. This means that we must address the individual secrecy concerns of numerous academic branches and instructors while also enhancing the overall quality of education delivery [74].

3.3.2 Business Cloud

E-commerce or state-owned banks with a large amount of data need more maintenance and support people to assist them in maintaining the system and dealing with any crises that may arise. The operations center, on the other hand, has the most important jurisdiction [72]. A further security concern that most individuals overlook in our country is using public wireless internet services to access their sensitive personal information. A free urban wifi network is available in the majority of significant cities. Most people aren't concerned with whether or not they are safe and secure until they begin to utilize them. It demonstrates that no encryption is used during the transmission of the data. Insecure data, such as financial or payment services, may be accessed by customers through the internet or their phones. Hackers may take advantage of these customers' negligent behaviors to obtain their payment authentication credentials in a matter of minutes [72][74]. The bandwidth, which is still incredibly small, is one more problem with the free network.

Possible users may lose contact during business transactions, leaving their private records more vulnerable to future aggression. Hundreds of online retailers and companies supply various 3-party API that are not entirely stable. Because of this, the environment is very susceptible to repeated cyberattacks by hackers. [72].

3.3.3 Mobile Cloud

The rise of cloud computing and the prevalence of smartphones have resulted in humans becoming more familiar with a new stage of the record-sharing concept. Information is kept on the mobile, and cloud devices are being used to recover files from the cloud. The growth of cloud technology and the widespread use of mobile phones, humans are gradually becoming familiar with a new stage of record-sharing in which the information is stored on the cloud rather than on a local hard drive. Using mobile devices, data may be stored and retrieved via cloud storage services [75].

Mobile devices often have finite storage and processing capability, while the cloud offers vast computing power and storage space. The CSP utilize to save and exchange info to achieve acceptable performance [75]. Different cloud mobile apps have widely used at this time. Individuals (data holders) may exchange their photographs, images, docs, and other records to the cloudin these applications and distribute data with other individuals they want to appoint.

Additionally, CSPs provide data management capabilities to information owners. Because owners have access to their private data, users may also choose to keep their statistics data public or share it exclusively with particular users. Many consumers are concerned about the privacy of sensitive information due to the vulnerability of mobile data kept in the cloud.

3.3.4 Healthcare Cloud

To achieve different health-related technologies, such as remote health monitoring, illness surveillance, and mature individuals are essential resources for healthcare research and commercial healthcare initiatives such as smartphones, watches and smart wristbands [76]. These devices produce massive amounts of private health information, which serve as valuable data for healthcare technology and practical uses.

Personal health data must be owned and controlled by the individual users. Typically, health data is controlled by several providers, suppliers of products, or is dispersed across multiple healthcare systems. By and large, it obstructs data exchange and curtails data security, since these centralized data warehouses and providers are appealing targets for cyber-attacks.

Several nations throughout the globe, such as Austria, have taken on the part of the e-healthcare security operations, such as the German electronic Health Card (eHC) system under development or the Taiwan Electronic Medical Record Template (TMT). A smartcard containing info (user name, medical insurance corporation) will be given to each policyholder in Germany.

The smartcard will allow policyholders to access and store medical data such as medication orders, basic first aid such as blood group, medical histories, and electronic health records (EHR). Smartcard integrated with cryptographic keys and features that enable the patient to identify sensitive data to be encrypted.

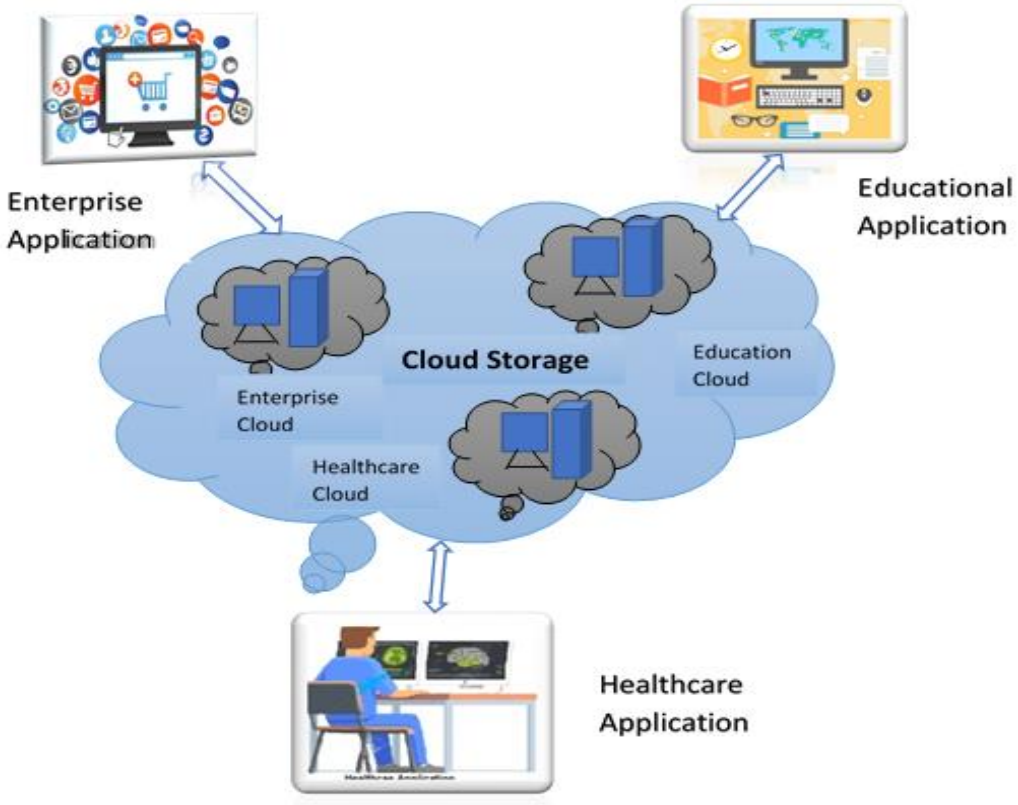

Figure 3.2 Storage Model

3.4 CLOUD STORAGE ISSUES

It's no wonder that businesses have hopped on a cloud platform with the rising prevalence of CC and its ever-increasing flexibility. A cloud server may be a versatile tool that not solely satisfies storage and process necessities however additionally helps to avoid wasting thousands of dollars in IT investment for the enterprise data [77]. The following are significant threats that need to be discussed when using company cloud storage and file sharing applications.

a. Out of control data

Organizations have had to take care of more recent security issues, such as the lack of sensitive information management, with cloud contributions such as "*Google Drive, Dropbox, and Microsoft Azure*" being routine business processes [78]. The issue is that, after third-party file-sharing services have been misused, information is often removed from the business's IT environment, putting the privacy settings of information out of the reach of corporate management, which is a serious concern.

b. Data Out Flow

Today’s, organizations are now putting more data and application in the cloud. The cloud has enabled businesses to become considerably more efficient, flexible, and quick to adopt new technologies due to use of these technologies. Most companies who have retreated from adopting the cloud have done so because of concern that their proprietary information would be leaked.

Because the cloud is a multi-user system in which all resources are shared, many people are concerned about their data security. In addition, it is a third-party service, implying that the distributor is potentially in danger of seeing or misusing personal information. It is quite natural to call into doubt the abilities of a third party. Data leaking may be caused by various external risks, including hostile breaches of cloud service providers and violations of online cloud accounts, among others [79].

Using a third party to store data relieves you of a lot of responsibility. But this has its drawbacks. If your storage provider suffers from outages or virus outbreaks, you will lose access to your data. The longer your data is unsecured, the greater the danger.

c. Snooping

Snooping is the unauthorized access to another's data. Snooping includes casually observing another's computer screen for e-mail. Files stored on the cloud is one of the most vulnerable withoutsecurity measures in place can be hacked. Additionally, the fact that hang on and transmitted over the net is a significant risk problem. And information can still be intercepted on the path to its destination, despite the cloud service offering cryptography for files. The excellent security structure of threats would have encrypted documents and transmitted over a tightly closed network it prevents outsiders fromaccessing metadata from the cloud [80].

d. Shared Servers

Cloud storage solutions continue to utilize servers to store data, but customers do not have physical access. Cloud storage companies do not develop dedicated servers for each user; instead, server capacity is shared as required across several clients. You might harm your data if those who access your servers submit possibly abnormal or harmful data.

e. Cloud Credentials

Connection to cloud-based applications, including AWS and the Microsoft Azure cloud, is handled by cloud identities. The primary business model of the cloud is that it provides everyone with almost limitless storage. An organization’s data is often handled alongside the data of other customers, resulting in the possibility of third-party data theft. Potentially reduced by the idea that internet access is limited depending on user identities; nevertheless, the identities saved in the cloud may vary based on the passwords used by different users, making certificates vulnerable to theft.

However, although a credential breach may not give hackers access to content within your folders, it may enable them to do other actions on your files, such as duplicating or removing them.

The only method to combat this security danger is to encrypt your sensitive data and safeguard your distinctive passwords, which may need the purchase of a secure password management system.

3.5 SUMMARY

Many cloud computing companies and users also do not trust cloud providers to keep their private data in public cloud storage owing to a lack of clarity about the protection of data transfer in cloud storage services. Primarily focused on security risks and problems different cloud platforms face (Education, Enterprise, and Healthcare). When organizations store data physically, high-cost hardware is required and purchased, and a lot of space is needed, and it takes more time. It concludes that today's global cloud computing is increasingly growing in the cloud industry. Businesses and organizations must store their massive data at a low cost. In order to maintain privacy, we must not sacrifice on security. For various reasons, data storage on the public cloud is much more beneficial than conventional storage, including accessibility, flexibility, efficiency, mobility, and compliance with required specifications. When it comes to protecting client information in the cloud, data centers and service providers have provided a certain level of protection for their companies and business data, even though more protection is needed for client information in cloud storage in terms of safety and anonymity.

CHAPTER-4

A NOVEL MONARCH BUTTERFLY OPTIMIZATION WITH ATTRIBUTE BASED ENCRYPTION FOR SECURE PUBLIC CLOUD STORAGE

This chapter Highlights valuable reports of file encryption and decryption time to secure public cloud data storage. It compares the throughput time for optimizing the security of cloud computing storage.

4.1 INTRODUCTION

Cloud technology is used by several platforms, including different approaches, and software architecture methodologies, among other aspects [81][82]. IaaS, PaaS, and SaaS are the three cloud services available using four cloud software deployment components. We may create framework solutions for private, public, hybrid, and community systems [83].

CC offers many advantages over traditional, modern computation or storage techniques, including accessibility, scalability, and adaptability. Despite this, the cloud computing environment has several security issues to contend with: (i) Client security issues have emerged and (ii) Cloud service companies are experiencing vulnerabilities. [84]. The study predicts numerous types of assaults connected to the strength AES (advanced encryption standard) technique, including separate damage detection attacks and present defects to the AES framework to regain access to secret information. [85].

The CC approach might also offer a few feasible service areas practices through computation resources that would be very efficient in social networking, telecommunication services, online services, and computing technology in other areas. Consequently, Cloud data centers should have a limited number of procedures capable of confirming the truthfulness of information and the completeness of storage that is maintained in the cloud [86]. Fig 4.1 illustrates the outline of security in CC atmosphere.

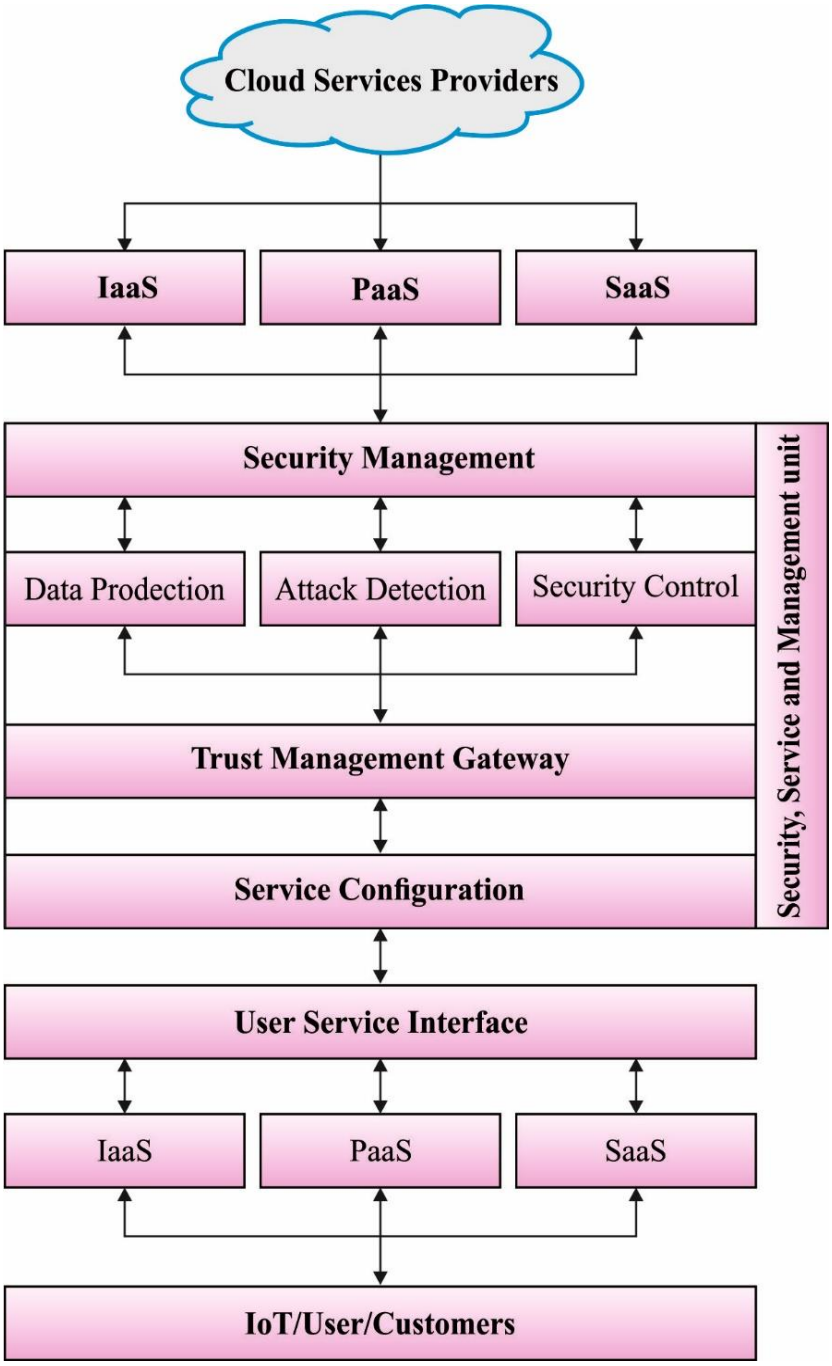

Figure 4.1 Overview of security in CC environment

Current security systems utilize more than one characteristic simultaneously, resulting in weaker security and more time consumption for encoding and decoding the data. It makes the operation more time-consuming and, as a result, increases network latency, network use, and power consumption [87]. As a result, the CSP provides security in conjunction with each characteristic, such as time consumption, decreased power usage, and network latency.

Previously, generally available methodologies were unable to correctly measure the security of cloud-based services, despite their widespread use. This design must use time, reduce power, decode, and postpone network consumption to grow information protection in CC. In CC, Attribute-Based Encryption (ABE) is a cryptographic technology often used to safeguard the security of a user's data security. Due to its higher-level advantages, such as cost reductions, simplicity, and scalability, cloud computing is being used in the majority of relevant areas. Because of its vulnerability, the development of a security approach is quite tricky; this would impact both the availability of resources and the economic advantage[88]. The attacker targets devices and mobile apps to increase the hypervisor's ability to defend against DoS and virtual machine side-channel assaults. The presence of traffic would impact the CC, in which case the case IP address used to eliminate the traffic from the network. Encouraging public auditing in this way is accomplished via the use of a privacy-preserving approach.

There are a certain number of blocks in the shared information, each containing the signer's identities, and the data is held secret from other parties until the shared data is authenticated. It is feasible to preserve saved data using a decentralized access control system that restricts decryption to valid users and a decentralized critical distribution method. All information will be saved in the cloud according to the access policy recognized by the cloud [6]. Virus, Trojan horses, the man in the middle attacks, back doors, and denials of service are only some of the network security threats that exist. Local sites are being converted to commercial, public clouds to gain flexibility and cost savings, and the organization will be compelled to outsource sophisticated data to achieve these goals.

The cloud checks the user's identification before storing the cloud data, making no assumptions about the user's identity. Authenticated users are able to decode the stored information and then perform modifications such as generation and reading in order to avoid spoofing. Monarch Butterfly Optimization with Attribute-Based Encryption (MBO-ABE) is a revolutionary approach for safe public cloud storage that is presented in this article. The suggested MBO-ABE approach aims to safeguard data stored in the public cloud to enhance the privacy of sensitive information. It is currently in beta testing.

The MBO algorithm, which is based on the migration of monarch butterflies, is used to the ABE approach to improving the security results obtained by the method. A thorough set of experiments conducted is carried out in order to ensure that the suggested MBO-ABE approach continues to improve.

4.2 MOTIVATION BEHIND THE WORK

This section examines the state-of-the-art encryption algorithms that have been created for cloud computing systems. R. Prathap, and Mohan Sundaram [89] proposed a two-sided decoding method that could be decoded by two entities (i.e., the receiver and a centralized agent), thereby increasing the data flow security by allowing the centralized agent to read the data transmission words during the decoding process. Deng et al. [90] formalized and developed an IBET module by integrating two well-known encryption techniques, IBE and IBBE. IBET authorizes and identifies data users for data access based on their recognizable identities, which prevents the need for complicated certificate administration in conventional secure distributed methods. Fun and colleagues [91] developed an extension to the Honey Encryption system for strengthening the security of storing files on the publicly CC. Honey Encryption adds a degree of security to the encrypted data by providing phony data in response to each incorrect assumption about the users' passwords made by the encryption algorithm. From the suspect's viewpoint, such fictitious data is identical to the actual data, increasing the complexity of password prediction.

Shen et.al. [92] developed a system for a multi-level cloud storage strategy, which was merged with AES symmetric key encryption as well as a more advanced identity-based PRE technique. A few strategies for building safe public key encryption systems against associated arbitrary nature attacks were presented by Liu [93], including the RRA-CPA secure public key encryption system, which uses an efficient decoding mechanism and a small ciphertext size. Veeraragavan and colleagues [94] suggested an EEA protect data stored in cloud storage. It makes use of the same key for both decoding and encoding the data that has been previously stored in the cloud. The results of the projected EEA created separate ciphertext for plaintext that was otherwise equivalent.

Krishnasamy and Venkatachalam [95] used a secure AP3DE approach to validate aggregate technological competence with assurance. Runhua Xu et al [new]. The CP-ABE-HP technique were proposed in this work, which successfully realizes policy that is buried behind encryption. The TMPD and data security container were suggested in the study based on the existing notion of a container. The operating outcomes of ES demonstrate that the technique makes it easier for users to do their tasks.

Yu, Y. Luo et al. [47] established a system for cloud computing data sharing that is both privacy-preserving and safe by combining CP- Attribute-Based Encryption with the IBE methodology, described in detail below. A fine-grained data access control mechanism is provided, and backward secrecy, safety compared to user cooperation with the cloud, support for user adding, overturning, and attribute changes in the proposed approach. The use of computational overhead necessitating the use of matching methods has been identified as a drawback.

4.3 PRELIMINARIES

4.3.1 CP-ABE

The KGC, encryption, and decryption functions are all included in the Cipher text Policy-Attribute Based Encryption (CP-ABE) paradigm. The KGC generates secret keys depending on the attributes of the individual. The encryption method encodes the communication by the access privileges that have been selected. The ciphertext is successfully decoded unless the secret key's attribute matches the comparable access policy's access policy. Inside the CPABE paradigm, there still are four different approaches:

1. Setup: Public variables *PP* and the master secret key *MSK* are both inputs to this algorithm.
2. Key_Gen: It receives *PP*, *MSK*, and the group of characteristics S as inputs and provides a secret key SEK_s that is identical to *S.*
3. Encoding: it takes *PP*, access policies *W,* and message *M* as input as well as output the ciphertext $CT_{W.}$

4. Decoding: it takes *PP*, CT_W and SK_S as input as well as output the message *M* only if the attribute S fulfill the $\mathbb{W}$; for occasion, $S \vDash \mathbb{W}$.

4.3.2 Oblivious Transfer (OT)

The OT protocols are two-party computation protocols in the sense that one party is the transmitting side ($\mathcal{S}$) and the other party is the receiving side ($\mathcal{R}$), respectively.

The procedure ensures that the following things happen: $\mathcal{R}$ receives the collection of messages sent by $\mathcal{S}$. $\mathcal{R}$ can get the division of these messages; but, $\mathcal{S}$ does not recognize that message as one that $\mathcal{R}$ has obtained. It is compared to a conventional c (OT_2^1)protocol setup [89]:

(1) $\mathcal{R}$ arbitrarily picks $\alpha, \beta, \gamma \in [1, q]$ and groups τ as tracks:

(a) If $\sigma = 0$, then $\tau = \left(g^{\alpha}, g^{\beta}, g^{\alpha\beta}, g^{\gamma}\right)$.

(b) If $\sigma = 1$, then $\tau = \left(g^{\alpha}, g^{\beta}, g^{\gamma}, g^{\alpha\beta}\right)$.

$\mathcal{R}$ directs τ to $\mathcal{S}$.

(2) $\mathcal{S}$ receives $= (\mathrm{x}, y, z_0, z_1)$. Afterward, $\mathcal{S}$ verifies $z_0 \neq z_1$. If not, its output $\perp$, and abandon.

Similarly, $\mathcal{S}$ picks $u_0, u_1, V_0, V_1 \in [1, q]$ arbitrarily and calculates the following 4 values: $\omega_0 = x^{u_0} \cdot g^{v_0}$,

$$k_0 = (z_0)^{u_0} \cdot y^{v_0} \quad (1)$$

$$\omega_1 = x^{u_1} \cdot g^{v_1},$$

$$k_1 = (z_1)^{u_1} \cdot y^{v_1}$$

Afterward, $\mathcal{S}$ computes $\mathrm{c}_0 = \mathrm{x}_0 \cdot k_0, c_1 = x_1 \cdot k_1$ and sends (ω_0, c_0) and (ω_1, c_1) to $\mathcal{R}$. Eventually, $\mathcal{R}$ computes $k_\sigma = (\omega_0)^{\beta}$ and attains $\delta_\sigma = c_\sigma \cdot (k_\sigma)^{-1}$

4.3.3 Bilinear Maps

Assume that $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$ be 3 q order cyclic group. The bilinear pairing function e is a bilinear map:$\mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, and fulfills the following properties:

(1) $\forall g \in \mathbb{G}_1$, $\forall h \in \mathbb{G}_2$, $\forall x, y \in Z_q^*$, there is $e(g^x, h^y) = e(g,h)^{xy}(2)\exists g_0 \in \mathbb{G}_1$, $\exists h_0 \in \mathbb{G}_2$, $e(g_0, h_0) \neq 1(3)\forall g \in \mathbb{G}_1$, $\forall h \in \mathbb{G}_2$, $e(g,h)$ is predictable in polynomial period.

It is used in the case of asymmetric bilinear groups; i.e, $\mathbb{G}_1 \neq \mathbb{G}_2$.

4.3.4 Security Assumption

Definition 1. Accept that $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$ process of bilinear group, undertake g be a creator of $\mathbb{G}_1$, and deliberate h be creator of $\mathbb{G}_2$. In order to few unknown $\alpha \in \mathbb{Z}_p^*$, regulate $g_i = g^{\alpha^i}$, and set $\vec{y}_{g,\alpha,n} = (g_1, \ldots, g_n, g_{n+2}, \ldots, g_{2n})$. It is almost a technique $\mathcal{B}$ resolves *n*- BDHE issue with profit ϵ if on input $g, h, \vec{y}_{g,\alpha,n}$,

$$|\Pr|\left[\mathcal{B}\left(e(\mathrm{g}_{\mathrm{n}+1}, h)\right) = 1\right] - \Pr[\mathcal{B}(Z) = 1] \geq \epsilon, \qquad (2)$$

where Z infers the random element of $\mathbb{G}_T^*$.

4.4 THE PROPOSED MBO-ABE TECHNIQUE

The recommended model, based on user contributions, allows AAC to obtain information about user attributes and critical recommendations. The fundamental paradigm of the proposed MBO-ABE approach is shown in Figure 4. 3. In practical applications, AAC is commonly conducted by an institution that certifies a personal attribute, such as a government agency, since it identifies the user's attribute individually and does not create any further leakage of the attribute. In other words, the blind token serves as proof that certain characteristics are owned by certain individuals. This token does not reveal any information about the user's qualities and is only used to verify the authenticity of the user. If the user wants assistance in acquiring their attribute key, they must send the blind token to KGC, a technical institute.

Following that, the user obtains the blind keys, and the secret key is removed from the local system, as illustrated in Fig. 4.2. The specific process as follows:

i. The client provides AAC with examples of their best qualities and most compelling proof.
ii. The AAC verifies the client's attributes and returns a blind token with signatures.
iii. To receive an attribute key, the client must send a blind token to KGC. The KGC couldn't access specific client attribute values. It just confirms that the client is compared.
iv. The KGC first checks the legality of tokens, and if the signature is invalid, it aborts the process. After that, it runs the key generation algorithm, which results in a blind key.
v. The customer acquires the blind key to KGC and has the private key removed from their possession.

ABE is a crypto technique that is widely used in CC to ensure the security of user data. These approaches have included multi-authority CP/ABE system with personality attribute revocation and the following strategies [90]:

Global Setup $(\lambda) \rightarrow GLP$. The global setup approach takes in security features and outputs a global variable GLP to work with.

Central Authority Setup $(GLP) \rightarrow (SEK*, PUK^*)$. A central authority uses this process using GLP as input to generate their unique secret key and public key pairs, which are denoted by the symbols SEK^*, PUK^*

Identity KeyGen $(GLP, RL, GID) \rightarrow K^*_{GID}$. The central authority runs this technique up on user requests to identity secret keys. It forms if the request is effective and when yes, creates K^*_{GID}.

Authority Setup $(GLP) \rightarrow (PUK, SEK)$. All attribute authorities use the authority establishment procedure using GP as input to generate their respective secret key and public key pairs. The key pairs are SEK and PUK.

KeyGen $(GLP, SEK, GID, i) \rightarrow K_{i,GID}$. The approach for generating attribute keys takes an identity GID,the global parameter, an attribute i corresponding to a few authorities, and the secret key SEK with this authority. It creates a K (i, GID) key for this attribute, identifier pair.

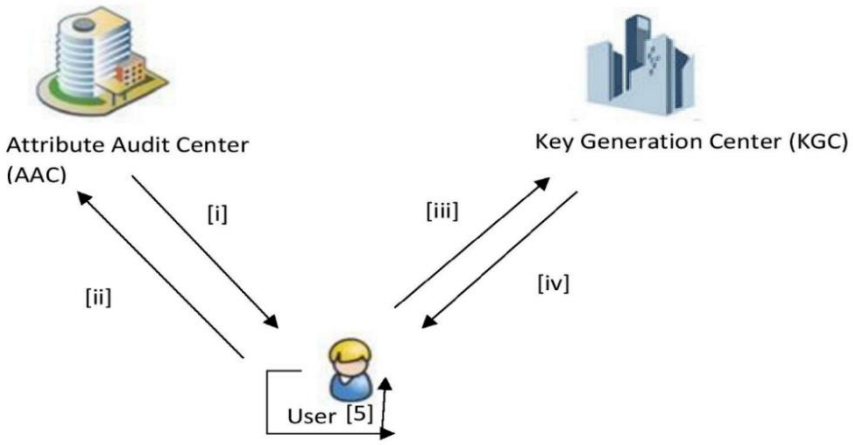

Figure 4.2 Blind key generation

Encrypt (GLP, $\mathcal{M}es$, (A, ρ), $\{PUK\}$, PUK^*, RL) $\rightarrow CT$. $\mathcal{M}es$ an access matrix (A, ρ), a set of public keys for significant authority, the public key of central authorities, a list of revoked users, and a global parameter are all inputs into the encrypted approach. A ciphertext CT produced by this programme.

Decrypt (GLP, CT, (A, ρ), $\{K_{i,GID}\}$, K^*_{GID}, RL) $\rightarrow \mathcal{M}es$. The decryption approach considers the global parameter, the revoked user lists, the *CT*, the identity key and the collection of keys comparable to attributes, identity pair each with the same stable identity *GID*, and the identity pair each with the same stable identity *GID*. Its outputs either the message *Mes* or null if the collection of attributes *i* satisfy the access matrix corresponding to *CT*. After that, decryption fails.

The MBO approach is used to expand the enhancement of the ABE technique, which was previously used. Generally speaking, the MBO method is a population-based approach that is recognized as belonging to the class of SI techniques that are mimicked as the performance of certain species with swarming tendencies.

As previously stated, the MBO provided by Wang et al. [98] was inspired by a kind of butterfly native to North America, and that is believed to be the beauty of their process because of its orange and black hues. The monarch butterfly, the most well butterflies in North America, is distinguished by its orange and black pattern, readily recognized. It is a milkweed butterfly belonging to the Nymphalidae group. Female and male monarchs have distinctive wing patterns that might use to distinguish them.

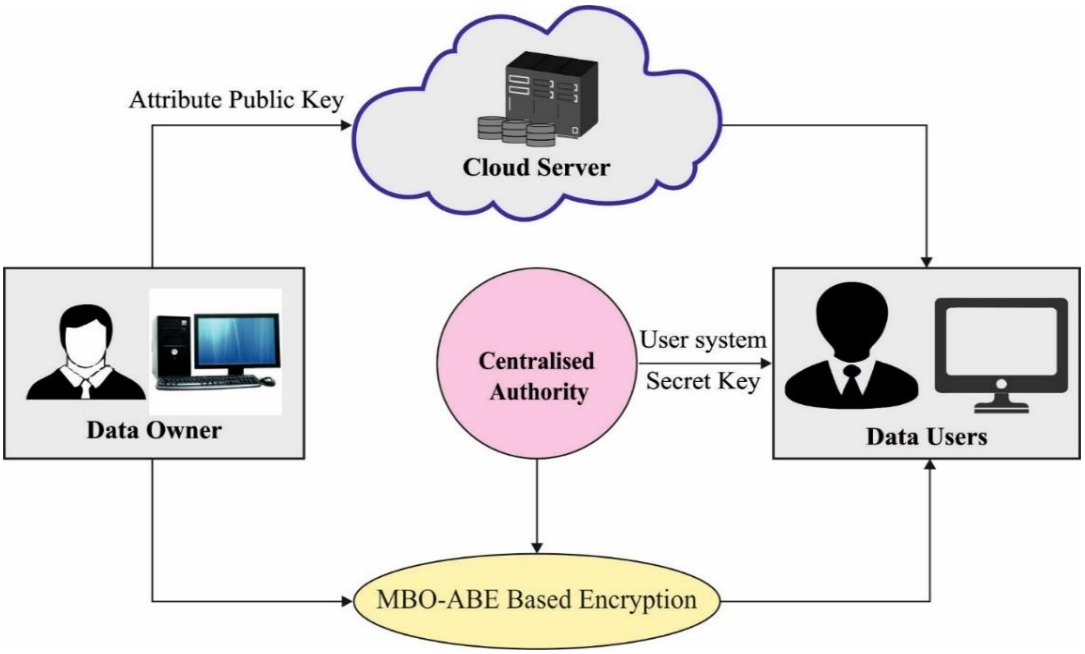

Figure 4.3 Overall process of proposed mode

Every summer, the eastern North American monarch is renowned for travelling hundreds of miles across the continent, from the United States and southern Canada to Mexico. It entails taking a flight from Colorado to California, which is west of the Rocky Mountains [52]. They travel hundreds of miles to Mexico in order to spend the winter there. Movements southward begin in August and are completed by the first frost of the season. When spring arrives, on the other hand, the inverse takes place. During these migrations, the females deposit eggs in order to produce offspring [53]. According to a recent study, certain butterflies engage in Levy flying throughout their migration or movement. A population management plan was developed to preserve the size of the population and limit the number of competence checks done on the butterflies. The total of the newly created butterflies formed in these two methods is equal to the original population.

The migratory performance of these butterflies serves as inspiration for the solution of many optimization problems [91].

Many guidelines and core models have been seen to be effective in achieving the best possible solution to problems:

1. Every butterfly that contributes to the creation of the population is also present in L 1 (home earlier in the migration season) or L 2 (home later in the migration season) (home next to migrate).
2. Each butterfly's offspring was formed using the migration function, regardless of whether the parents existed in L 1 or L 2.
3. FF eliminates 2 (either the unique kid or the parent) since the population cannot change and must be constant at all times.
4. The butterflies selected based on FF are admitted into the following generation, and their migratory function is not changed.

A butterfly's migrate function is expressed as.:

$$X_{i,j}^{t+1} = X_{r1.k}^{t} \tag{3}$$

where $X_{i,j}^{t+1}$ indicates the *K*th part *Xi at* $t+1$ peers that dispatched the area of butterflies i, and $X_{r1.k}^{t}$ designates the *K*th part of novel peers' area. At this point, r signifies the arbitrary amount figured as a formula:

$$R = rand * peri \tag{4}$$

Where $peri$ stands for the migration period time [92].

If, on the other hand, r>p, the location following the Kth element of the new generation is calculated as a formula after the Kth element of novel generation.

$$X_{i,j}^{t+1} = X_{r2.k}^{t} \tag{5}$$

Where $X_{r2.k}^{t}$ denotes the K^{th} element of *Xr*2 at t generation of butterfly *r*2. So that P demonstrates the ratio of monarch butterfly in L1.

A butterfly adjustment operator balances different migration strategies as they go from L 1 to L 2. Adjusting the P-value ratio is the key to achieving this goal. There are more butterflies in L 1 than in L 2; hence P is significant if P is more than or equal to the number of butterflies in L 1. The butterfly's location is changed when the rand generated is less than or equal to the value of P.

The following formula demonstrates how butterflies have been elevated to a more prominent position:

$$X_{j.k}^{t+1} = X_{best.k}^{t} \tag{6}$$

Here, the Kth element of Xj at the current generation t in both L 1 and L 2 is denoted by *Xj* at $t + 1$, and the Kth element of *Xbest* the current generation t in both L 1 and L 2 is denoted by $X_{best.k}^{t}$.

When r and $>P$ is reached at this stage, it may be elevated to the status of the formula.

$$X_{i,j}^{t+1} = X_{r3.k}^{t} \tag{7}$$

In contrast, since rand suggests that BAR is better, the unique location was elevated to the status of the formula:

$$X_{j.k}^{t+1} = X_{j.k}^{t+1} + \alpha * (dx_k - 0.5) \tag{8}$$

Where BAR denotes the butterfly modification rate, and dx denotes the walk step of j butterflies calculated as carrying out Lévy flight as:

$$(Dx = Lévy(X_j^t) \tag{9}$$

α in Eq. (8) denotes the weighted factor which is estimated as formula:

$$\alpha = S_{\max} = t^2 \tag{10}$$

S max indicates the maximum amount of time that butterflies may travel in a single stride, and t indicates the number of generations currently in existence. In Figure 4.4, you can see the flowchart of MBO in action.

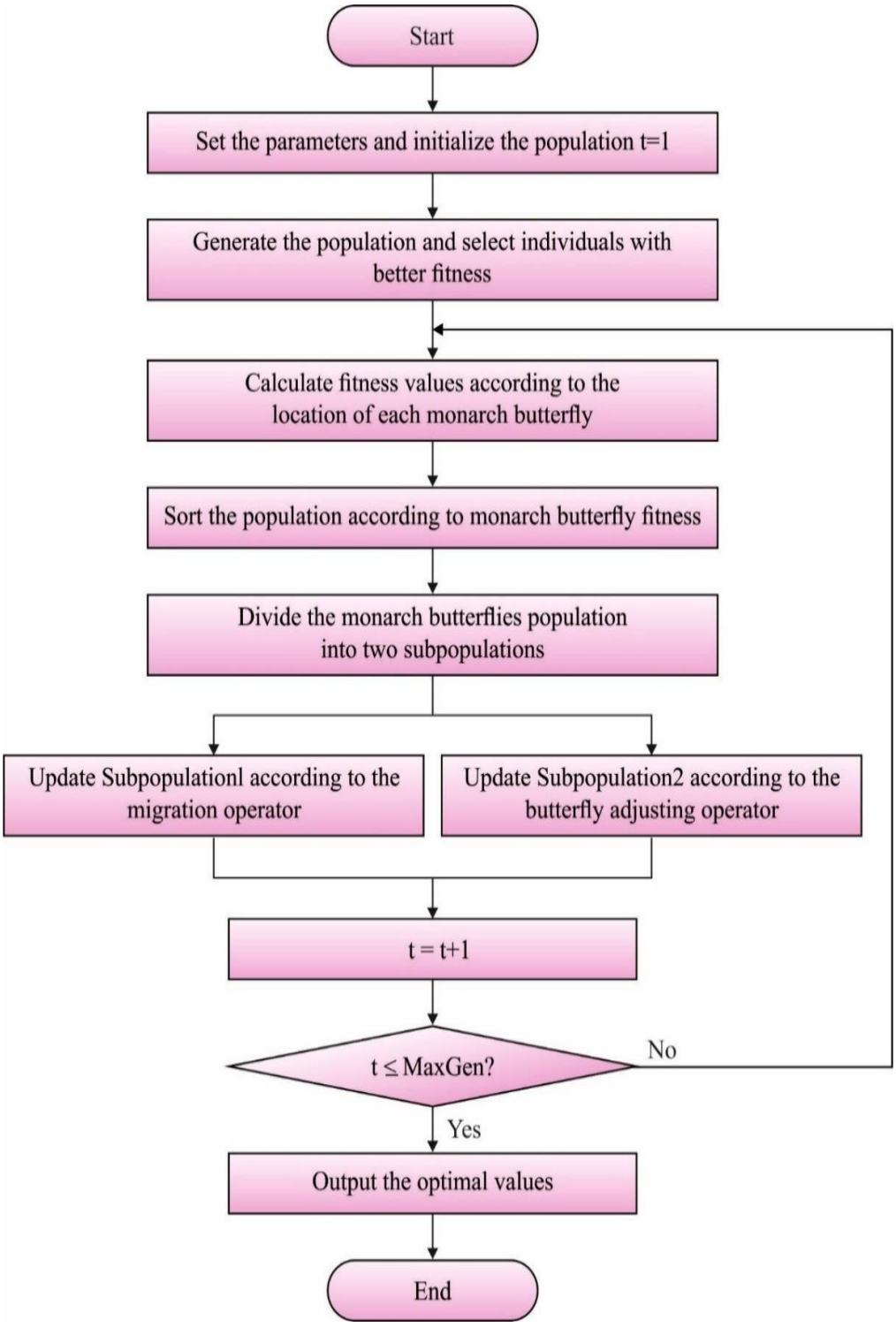

Figure 4.4 Schematic flow diagram MBO algorithm

4.5 PERFORMANCE VALIDATION

This section investigates the overall performance of the suggested MBO-ABE approach in terms of several different aspects.

Encryption Time (sec)			
File Size (GB)	MBO-ABE	BH-WABE	HABE
1	105	118	132
2	212	230	250
3	322	341	362
Decryption Time (sec)			
File Size (GB)	MBO-ABE	BH-WABE	HABE
1	102	113	123
2	200	221	262
3	524	598	625
Throughput			
File Size (GB)	MBO-ABE	BH-WABE	HABE
1	0.00952	0.00847	0.00758
2	0.00943	0.00869	0.00800
3	0.00932	0.00874	0.00828

Table 4.1 MBO-ABE technique outcome analyses of encryption and decryption time.

Table 4.1 illustrates the encryption and decryption time details of the proposed MBO-ABE approach for files of variable sizes under various conditions. According to the results of a performance investigation, the MBO-ABE approach achieved maximum throughputs of 0.00952, 0.00943, and 0.00932 for file sizes ranging from 1-3GB, correspondingly.

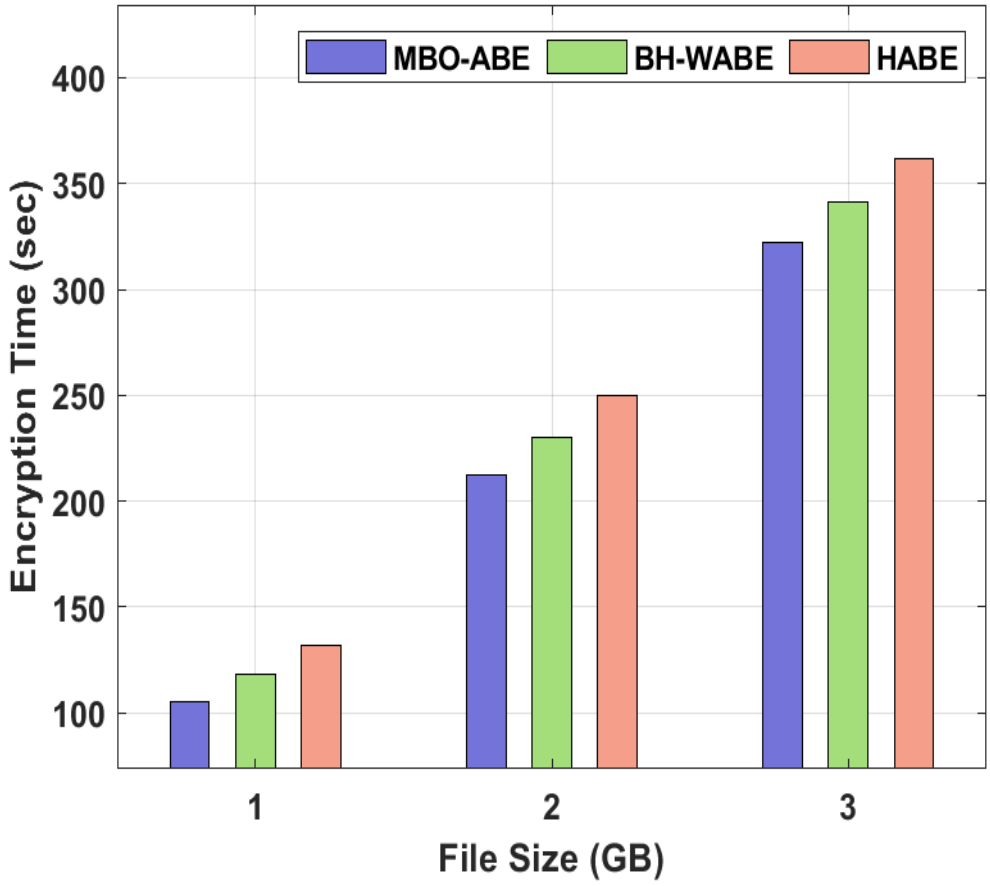

Figure 4.5 Encryption time investigation of MBO-ABE model

The encryption time analysis of the MBO-ABE approach compared to other algorithms is shown in Fig. 4.5 for three different file sizes. The MBO-ABE approach, as seen in the picture, takes less encryption tome than the other ways, which is advantageous. With a 1GB file size, the MBO-ABE approach has exhibited a minimum encryption time of 105s; both the BH-WABE and HABE techniques demonstrated a more excellent encryption time of 118s and 132s, respectively, with the same file size. The MBO-ABE technique, with a file size of 3GB, has provided a minimum encryption time of 322s. Still, the BH-WABE and HABE algorithms, with file sizes of 3GB, have provided a superior encryption time of 341s and 362s, respectively.

Figure 4.6 compares the decryption time of the MBO-ABE method with the decryption times of other methods for three different file sizes. according to the figure, the MBO-ABE approach surpassed the other ways in that it requires the least amount of decryption time.

For example, with a 1GB file size, the MBO-ABE approach has shown a faster decryption time of 102s, while the BH-WABE and HABE techniques have demonstrated faster decryption times of 113s and 123s, respectively, with the same file size.

Similarly, with a file size of 3GB, the MBO-ABE technique has proven a minimum decryption time of 524s. Still, the BH-WABE and HABE approaches have exhibited a more excellent decryption time of 598s and 625s, respectively, with the same file size.

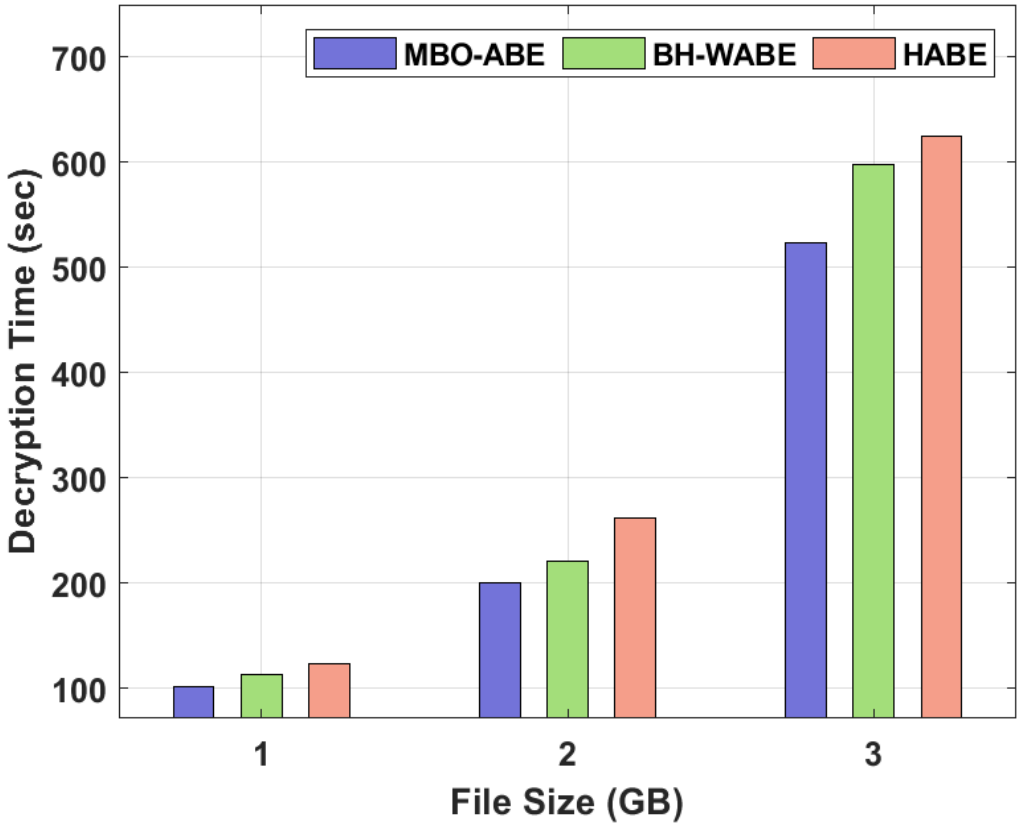

Figure 4.6 Decryption time investigation of MBO-ABE model

Table 4.2 illustrates the User key generation time (UKGT) and the storage cost of secret key (SCSK) analysis of the suggested MBO-ABE method under various weighted characteristics. Fig. 4.7 shows the UKGT time analysis of the MBO-ABE approach compared to other methods when the number of weighted attributes is increased. The figure shows that the MBO-ABE technique requires the least amount of UKGT time matched to the other algorithms.

The MBO-ABE method, for example, has a lower UKGT time of 0.63s with weighted attributes of 10, but the BH-WABE and HABE methods have produced a better UKGT time of 1.00s and 1.50s, respectively.

User Key Generation Time (s)			
Count of Weighted Attributes	MBO-ABE	BH-WABE	HABE
10	0.63	1.00	1.50
20	1.13	1.61	2.50
30	1.67	2.50	3.00
40	1.94	2.80	4.00
50	2.39	3.50	5.50
Storage Cost of Secret Key (KB)			
Count of Weighted Attributes	MBO-ABE	BH-WABE	HABE
10	1	2	3
20	2	3	6
30	3	4	8
40	4	6	10
50	6	8	13

Table 4.2 Result analysis of MBO-ABE model under User key generation and storage-follow encryption time

However, when using the weighted attributes of 50, the MBO-ABE methodology has exhibited a minimum UKGT time of 2.39s. Still, the BH-WABE and HABE techniques have proven a better UKGT time of 3.50s and 5.50s, respectively. A comparison of the MBO-ABE method with other methodologies is shown in Figure 4.8, where the number of weighted characteristics is shown as a percentage in total. It can be seen in the picture that the MBO-ABE method takes less SCSK time than the other two methods.

For example, while using the weighted attributes of 10, the MBO-ABE technique has provided a minimal SCSK time of 1KB. However, the BH-WABE and HABE approaches have improved SCSK time of 2KB and 3KB, respectively.

Following that, with weighted attributes of 50, the MBO-ABE approach has shown a minimum SCSK time of 6KB. In comparison, the BH-WABE and HABE algorithms have demonstrated a maximum SCSK time of 8KB and 13KB, respectively, using the same weighted attributes.

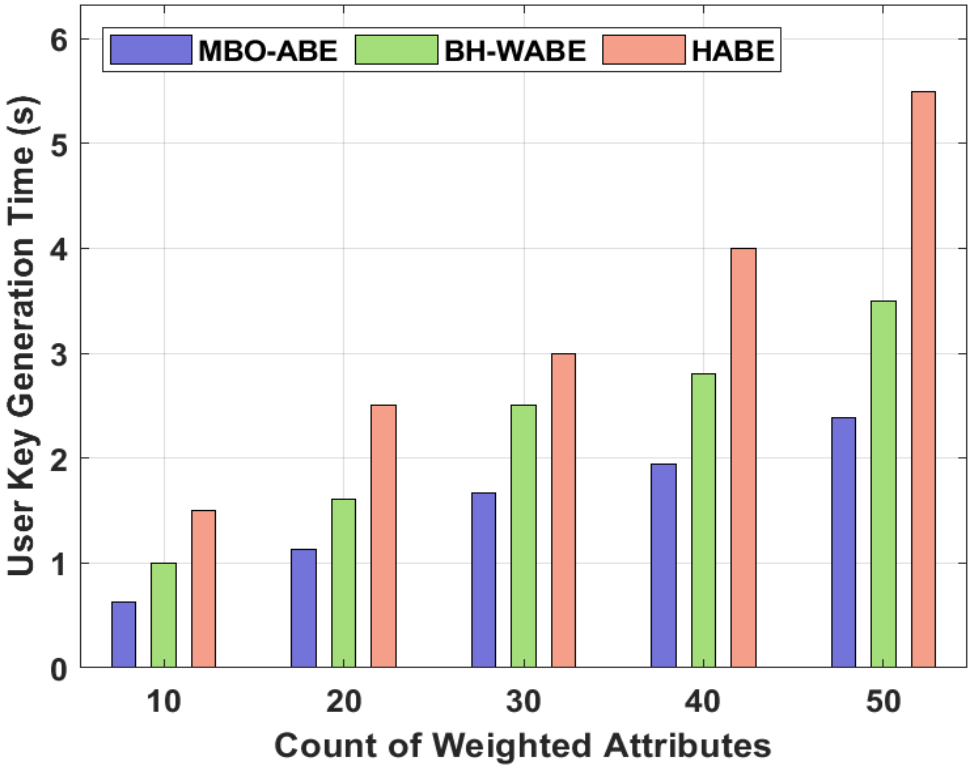

Figure 4.7 UKGT analysis of MBO-ABE model

The figure shows that the MBO-ABE technique requires the least UKGT time compared to the other algorithms. By way of illustration, while using the weighted attributes of 10, the MBO-ABE method has produced a lower UKGT time of 0.63s while the BH-WABE and HABE procedures have delivered a better UKGT time 1.00s and 1.50s, respectively. When using 50 weighted attributes, the MBO-ABE methodology has a minimum UKGT time of 2.39s, but the BH-WABE and HABE techniques have better UKGT times of 3.50s and 5.50s, respectively.

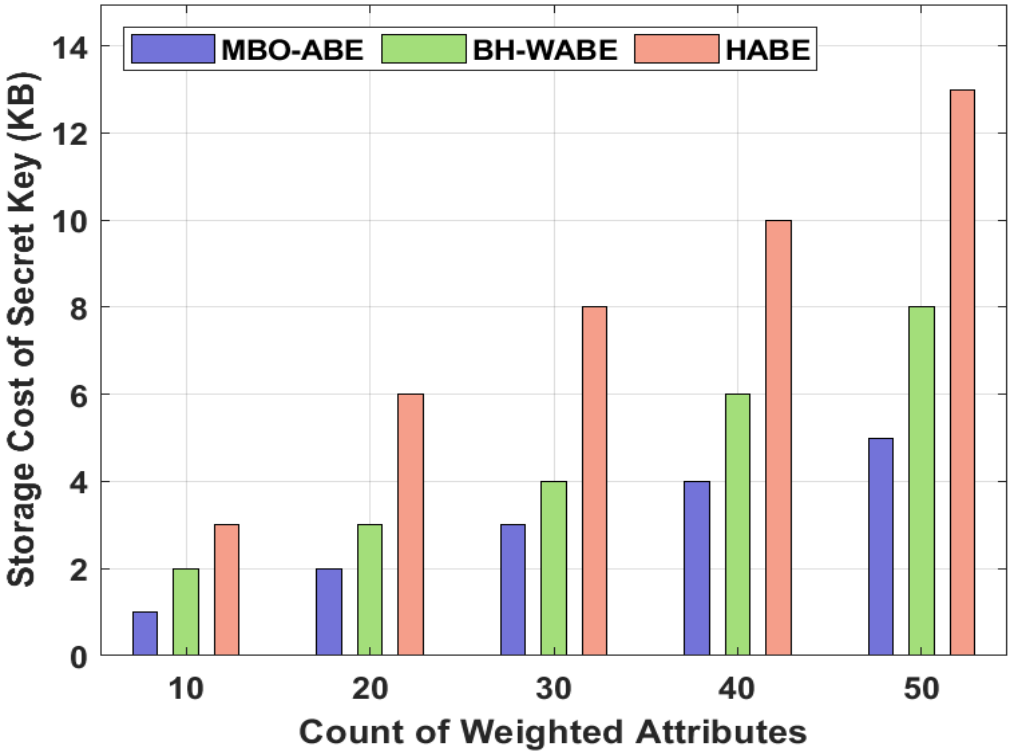

Figure 4.8 SCSK analysis of MBO-ABE model

4.6 SUMMARY

Cloud computing (CC) technology allows for the efficient use of existing physical resources via virtualization in a distributed computing environment where many users share a typical underlying physical hardware architecture. The ideas of CC are used to provide a collection of distributed, scalable, and elastic computing resources to clients through a high-speed Internet connection. Even while conventional public key encryption methods are used to ensure data security, they are unlikely to lead to more effective information exchange. Additionally, attribute-based encryption (ABE) is being developed as a crucial approach to providing security while also establishing good data transfer in a parallel manner, both of which are important. The ABE is a well-known cryptographic mechanism used to save the user's private information in CC. However, owing to the computational complexity and the possibility of decryption key leaks, it is not practical to utilize it in cloud storage. This study presents a unique monarch butterfly optimization with attribute-based encryption (MBO-ABE) approach for achieving security in public cloud storage systems based on monarch butterfly optimization.

The suggested MBO-ABE approach aims to provide safe data storage in public cloud storage to improve the confidentiality of sensitive data stored in the cloud. The MBO algorithm, which is based on the migration of monarch butterflies, is used to the ABE approach to improving the security results obtained by the technique. A comprehensive set of experimental evaluations is carried out to demonstrate the better results of the MBO-ABE approach that has been provided. Experiment results demonstrated that the MBO-ABE methodology outperformed the most current state-of-the-art technologies, as shown by the experimental values obtained.

CHAPTER 5

OPTIMIZATION OF SECURITY IN PUBLIC CLOUD STORAGE USING PARALLEL CHUNK ENCRYPTION SCHEME

This chapter introduces a Parallel Chunk Encryption (PCE) scheme, which provides public cloud data storage security. In order to secure, this scheme utilizes Trusted Third-Party Audit while secure cloud storage. Cipher Block Chaining (CBC) and AES techniques are used to achieve high-security goals. The Parallel Chunk Encryption Scheme gives efficiency and security on public cloud data storage.

5.1 INTRODUCTION

Cloud technology has grown famous due to its service capacity, availability, expandability, and low cost gained good popularity in a few years. Cloud computing is named as the cloud, cloud server hosting and cloud hosting. Cloud computing is similar to traditional hosting but allows users to store large amounts of data from any portion of the world over any communication resources in cloud storage and use it when required. Everything involves data, and most of the things we deal with in our everyday lives require cloud computing. Stuff like posting on Facebook or uploading the file onto Google Drive and you are using public cloud storage [93].

Enterprises can hire cloud services for storing their data and software with ease (e.g., No software installation on each device). The data stored on a cloud can be used by an employee anywhere and at any time. Several security algorithms are proposed, the trade-offs made between safety and efficiency warrant more improvement study [94]. In computer security, cryptography algorithm thrills a vigorous role in safeguarding complex data in the cloud; two cryptographic methods are symmetric and Asymmetric cryptography [95]. Block cipher mode Cipher Block Chaining (CBC) provides parallel data encryption using the previous block cypher [31]. Therefore, confidentiality and truthfulness of the data kept on the cloud should be considered essential requirements from the user's point of view. Figure 5.1 indicates cloud storage infrastructure included customers, cloud servers, and TTPA (Trusted Third-Party Auditor) in a cloud environment.

The customer saves data to the cloud service provider's storage space (CSP) [96]. TTPA periodically reviews user data and confirms the accuracy of the data, and TTPA notifies users when there is a disparity or assault on the user's data. TTPA should have the option of inspecting the cloud data professionally without demanding the neighboring backup of information. Specifically, our idea to take steps to encapsulate the following aspects: the first one to facilitate the public audit framework for information storage protection in cloud and to include a privacy audit system. Secondly, cluster auditing, in which-h the TTPA will concurrently perform multiple delegated audit tasks from different users.

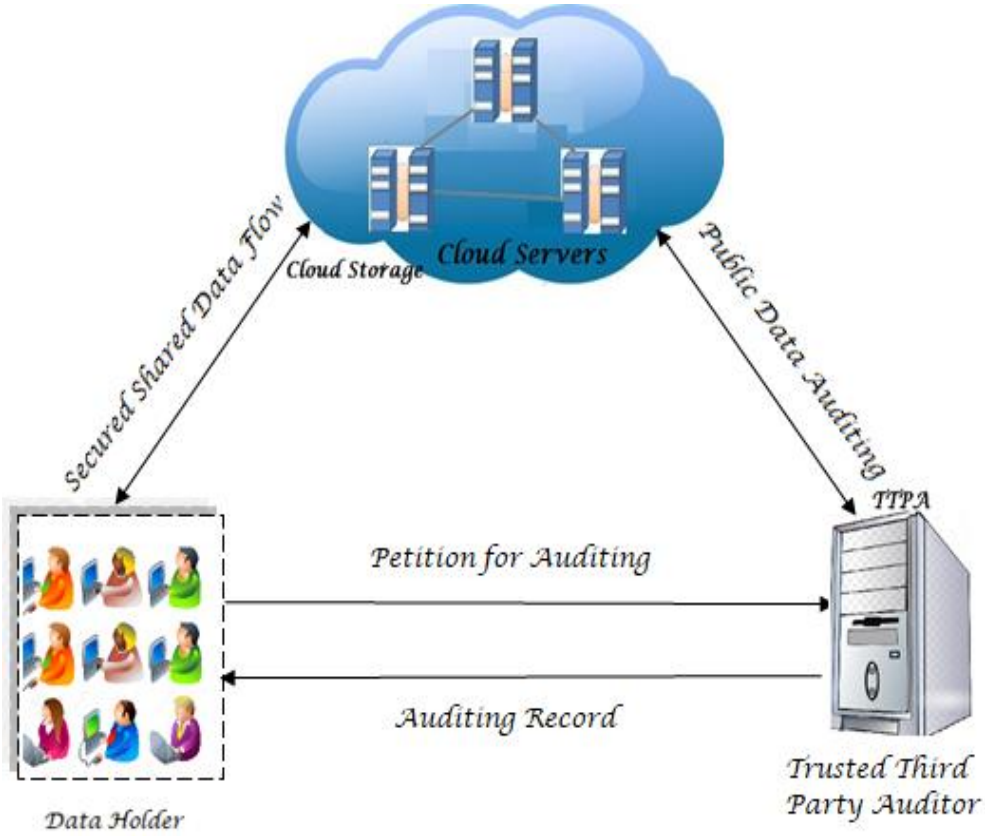

Figure 5.1 Cloud Data Storage Architecture

Section 2 discusses the recent cloud security challenges in public cloud storage and the methodology required to enhance the recommended scheme presented in section 3. Part 4 discusses the suggested work and the experimental result presented in section 5, lastly stating the conclusion of our offered work in section 6.

5.2 RECENT SECURITY CHALLENGES IN PUBLIC CLOUD

Service providers such as Amazon Web Services, Microsoft Azure, and Google Cloud Platform need to extend security services because of cloud computing, the rapid speed of advantages for enterprises by increasing performance, greater scalability, and enhanced acuteness. Eventually, inside the cloud environment, the user must protect their data.

In a 2020 cloud security report, the findings are a continuation of past challenges in the shared responsibility model to protect cloud data, cloud storage, and service providers such as Amazon Web Services, Microsoft Azure, and Google Cloud Platform need to extend security services because of cloud computing, the rapid speed of advantages for enterprises by increasing performance, greater scalability, and enhanced acuteness. Eventually, inside the cloud environment, the user must protect their data. In a 2020 cloud security report, the findings are a continuation of past challenges in the shared responsibility model to protect cloud data, cloud storage, and service.

1. 64% data loss and leakage are the highest cloud security concern for a cyber-security professional.
2. 42% Inadequate access control systems and abuse of user permits through unauthorized access the survey this year ranks number one as the single greatest perceived danger to cloud safety.
3. Cloud platform misconfigurations accounted for 40 percent.
4. Two most operations, security problem struggling SOC teams such as compliance (34%) and lack of visibility (33%) to infrastructure security.

Organizations recognize several key advantages of locating a cloud-based security solution; Respondents can select cost saving and faster time deployment and performance these top 3 factors to select cloud-based security solutions. Data security, security risk, and compliance and, lack of qualified staff in an organization is an overall obstacle to adopting cloud computing in 2019. According to recent challenges, data loss and leakage have a high degree of risks. As per our investigation of an existing algorithm and model, public cloud storage requires security optimization.

A new scheme has been developed to protect the secrecy of organization data stored in the public cloud.

Security Controversy	**Percentage of security issues**
Data loss and leakage	64%
Access control	42%
Interface and API	42%
Platform Mis-	40%
Infrastructure visibility	33%
Compliance	34%

Table1 5.1 A recent survey based on cloud security[97]

5.3 METHODOLOGY

It is sensibly impracticable to assess all the available literature correlated with security and privacy in public cloud storage. After picking source articles, conducted a literature study to identify several solutions models. In order to judiciously review an article downloaded a mixture of an article from Elsevier, the research gate, and the IEEE digital library is sensibly impracticable to assess all the available literature correlated with security and privacy in public cloud storage.

What is furthermore? Mainly, reviewed the articles by investigative and searching vigour each method acquires to identify solutions to the security challenges in public cloud storage. Finally, suggest the route of resisting cloud data protection.

Research Questions

In the escorting, concerns were presented in research to continue this investigation.

1. How can we protect data stored in the cloud?
2. What are further directions to move on parallel encryption along with cryptography?

The induction of our proposed scheme came from the modern cryptographic algorithm with a 512 bit key in AES to secure cloud data storage [98]. This suggested method takes computation time considerably high, which induced a new concept to reduce competition time without violating security.

5.4 RELATED WORK

This segment reviews related research on the confidentiality and integrity of public cloud storage and parallel encryption.

Imad El Ghoubach, et al [99]. An audit scheme proposed that offers users an effective and safe method for auditing their outsourced results. The proposed framework has a low user computation overhead. It allows them to select the process of input validation to a third party while retaining a low overhead of computation and communication without compromising the validity of the information stored also shows that our system can guarantee the integrity of data while being protected from forging and substitution attacks without violating the privacy of stored data. Biwen Chen, Biwen et al [100]. This article introduced a new cryptographic primitive, parallel and forwarded remote search public-key authentication, comparable search efficiency with the searchable symmetric encryption schemes. The proposed method attains parallelism mutually and forwards privacy at the disadvantage of marginally more significant storage costs. In [101], authors proposed increasing data storage security in cloud mistreatment Certificate less open monitoring theme. It is used to assure the protection related to the integrity of knowledge and information storage information in Cloud Computing. Even though KGC can produce a whole new partial key that will not violate the user's non-public key, there is still room for development in the area of preserving security and integrity in a significant way.

Rady, Mai et al. [102]. The authors provided an outline of assorted science algorithms that supported different outsourced information security schemes and authentication of queries. A new pre-processing architecture has been proposed. It attains the privacy and integrity of expanded databases query performance and data and database services (DaaS, DBaaS). The widespread adoption of these services still faces challenges. They said data protection is the most critical problem.

Bentajer, Ahmed et al [103]. The primary intention is to protect outsourced information with minimum keys, cryptographic keys, and high privacy management; the IBE mechanism provides additional security and flexibility within the control of top-secret keys. Moreover, at any time, cloud users will access encrypted information at any place. Dropbox, a model of the proposed design, was implemented to show its usefulness. A prototype of the proposed Dropbox concept is launched, but cloud providers are more likely to communicate only with low storage mobile devices. The experimental aims to calculate the amount of runtime (in seconds) of plain documents uploading and downloading actions for varying lengths.

5.5 PROPOSED PCE SCHEME

This section discusses the proposed Parallel Chunk Encryption (PCE) scheme, based on the parallel encryption mode with CBC [95] and Figure 5.2.

5.5.1 System Model

As shown in the following Figure 2: Three individuals, namely the data owners, cloud server storage, and TTPA (Trusted Third Party Audit) included in the security model as shown in Figure 2. First, data holders split the client documents (file, photos, and videos) into fixed-size chunks, then encrypt those chunks using our proposed scheme, Parallel Chunk Encryption (PCE); the cloud server stores encrypted chunks of documents.

TTPA will get an enciphered chunk from the cloud server for a data verification purpose. TTPA generates a hash code with the help of SHA-2 for each chunk and develops a digital signature on it when the client or data holder appeals for data auditing to the TTPA [5], the data holders directly request an enciphered chunk from the cloud server and produces the mess code for respective chunk consuming the similar SHA-2 process, then combines those hash codes and generates a digital signature. One signature generated by TTPA and one more signature generated by the data holder be compared by the TTPA in the signature verification process. If both are identical, then unharmed and no stranger or an intruder interferes with data. If both signatures are not similar, specify that the data integrity has been affected or harmed.

The forward encipher technique says forward the generated ciphertext to the next chunk to perform the XOR operation in the PCE scheme; the forwarding procedure continues to reach the last chunk in Plaintext. The previously encrypted chunk is input for the subsequent chunk encryption.

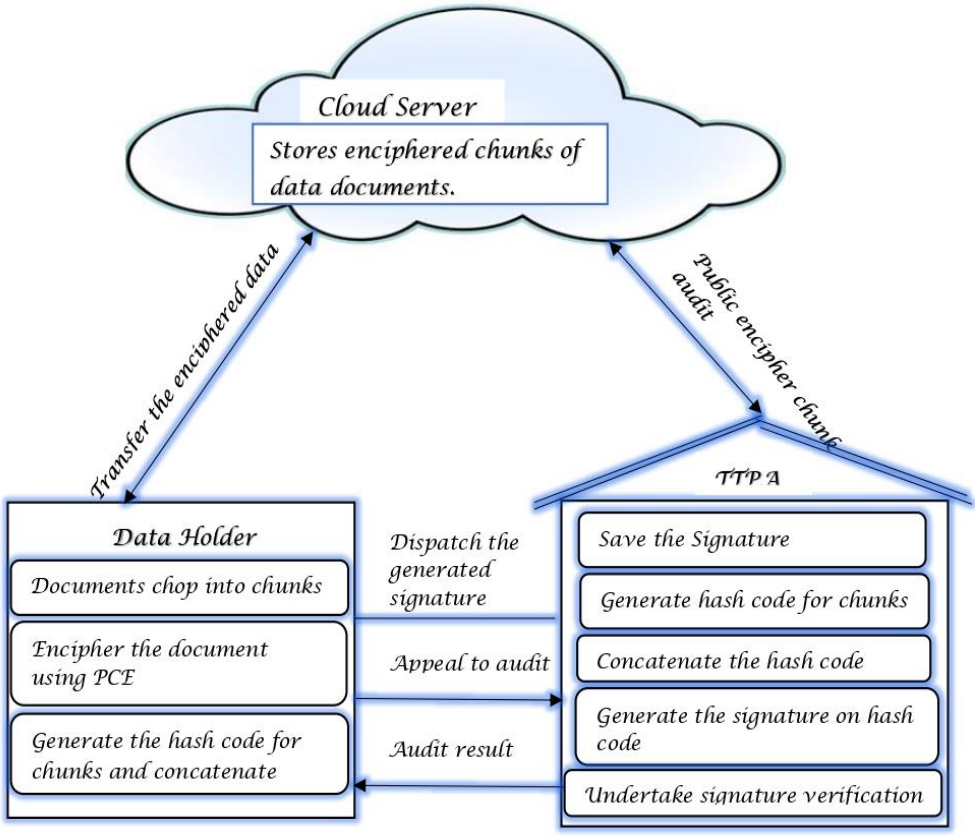

Figure 5.2 Proposed security Model

5.5.2 PCE Scheme level operation

In figure 5.3 shown, our proposed scheme PCE involves 2 phases: split the document and chunk encryption. Mainly document split divides document data into fixed-size chunks, each chunk size 128bits. Before the encryption of each chunk, the XOR operation was carried out using a Forward Encipher technique. The input for the first chunk XOR operation is Initialization Vector (IV) and chunk1. The output of the XOR operation is input for an encryption algorithm (AES) after encryption produces a ciphertext C1.

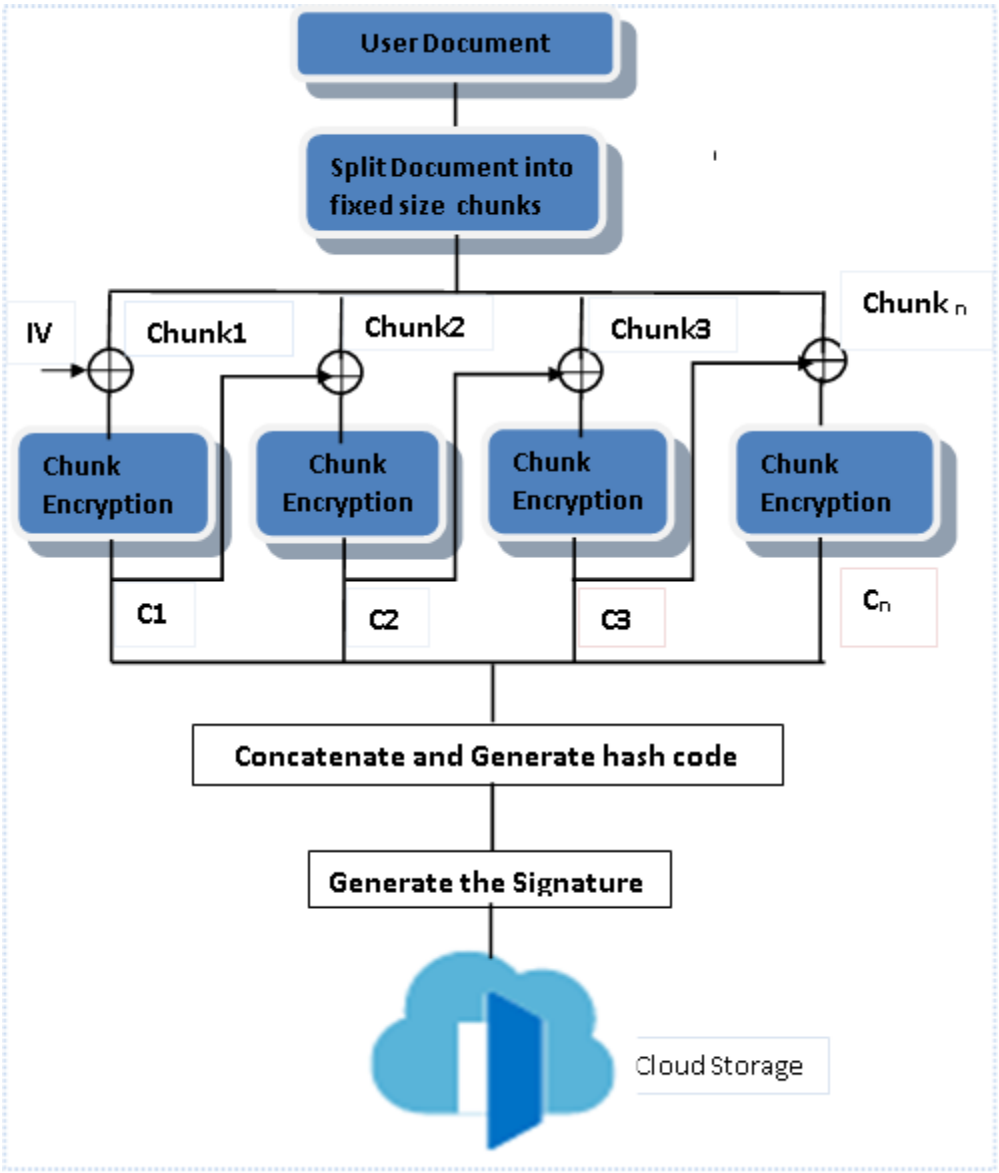

Figure 5.3 Structure of Parallel Chunk Encryption

The C1 is one input for the chunk2 XOR operation. This cycle continues until the last chunk ($Chunk_n$) gets enciphered. Initialization Vector (IV) is a stream of characters or a random number, which is the same as the chunk size. Initialization Vector is used during the first chunk XOR operation and makes each message unique. It adds complexity to the process hence the attacker can't easily break the messages. All encrypted chunk called ciphertext it's represented as C1- - -Cn; finally, all encrypted chunks called ciphertext it's represented as C1- - -Cn Finally, the encrypted chunks are stored in cloud servers.

5.5.3 Forward Encipher Technique

This technique says forward the generated ciphertext to the next chunk to perform the XOR operation in the PCE scheme; the forwarding procedure continues to reach the last chunk in Plaintext. The previously encrypted chunk is input for the next chunk encryption.

Encipher Algorithm: Encrypt plaintext Chunk

Procedure PCE_Encrypt (Msg, b_size)

1. $If\ Msg > b\_Size$ Then
2. $P\_Chunk[\,] < -Msg.split\ (b_{size})$
3. Random block of text IV

   $IV < -vector[\,]$ /* Initialization vector for first chunk P_Chunk1 */
4. DETERMINE Int_value1

   $Int_value1 < -$IV XOR P_Chunk1
5. Encrypt the Int_value _n using AES algorithm with 128bit key

   State=InitState (Int_value$_n$, key)

   AddRoundKey (state, Key0)

   for i =1 step 1 to 9

   SubBytes(state)

   ShiftRow(state)

   MixColums(state)

   AddRoundKey (state, key$_n$)

   end for

   SubBytes(state)

   ShiftRow(state)

   AddKey (state, Key$_{n-1}$)
6. DETERMINE Int_value2

   $Int\_value2 <$ C1 XOR P_Chunk2
7. REPEAT: Step 6 to encrypt plain text P_chunk2
8. Redo the process of step 5 and step 6 until all P_Chunk$_n$ gets encrypted.

The proposed Encipher algorithm encrypts the plain text. In Step2: The given document data is divided into a fixed-sized chunk every chunk size is 128bit (128 bits= 16 bytes). Step3 and 4: Generate initialization vector (IV) to perform the XOR operation with the first chunk.

$$Int\_value1 < -\text{IV XOR P\_Chunk1}$$

It produces intermediate value Int_value1. Step5: Encrypt an Int_value1 using AES algorithm with 128bit key the results in C1 ciphertext, key length based on a number of the round in AES. Every match produces a much more complex outcome, with byte substitution altering data in a nonlinear way. In terms of encryption, obscure the relationship between plaintext and encrypted text because of shift rows and mixed columns. Step6: The chunk2 XOR operation carries out using the previous chunk ciphertext C1 such that one input for XOR operation is Chunk2 'P_Chunk2' another on C1 the result of the XOR operation is 'Int_Value2' Int_value2<C1 XOR P_Chunk2 then chunk2 encrypted using Int_value2 with 128bit key, In step7 the encryption process is accomplished by repeating step 6. Step8: repeat step6 and step 7 until P_Chunkn gets encrypted.

Decipher Algorithm: Decrypt Ciphertext Chunk

Procedure PCE_ Decrypt (Cn , b_size , IV , e, d)

1. Decipher Chunk Cn using AES algorithm with secret key Kn
2. Accomplish XOR operation

$$P\_Chunk_n < -Int\_value_n XOR\ Cn - 1$$

3. Perform XOR operation on first Ciphertext C1

Calculate $P\_Chunk_1 < -Int\_value_n XOR\ Cn - 1$

4. REPEAT: The process of step2 and step3 until decrypting Cn ciphertext.

In parallel, the decryption algorithm decrypts the encrypted chunk, Step1: decrypts the ciphertext Cn can use an AES decryption algorithm that returns Int_valuen, Step2: perform XOR operation with an intermediate value with Cn-1 ciphertext will produce an original plaintext chunk using

$$P\_Chunk_n < -Int\_value_n XOR\ Cn - 1$$

Step3: Calculate plaintext for a Ciphertext C1 XOR operation carried out with intermediate value Int_value1. Parallel Chunk Encryption provides more security because of the forward encipher technique used in encrypting and decrypting processes.

The suggested algorithm simplicity by splitting a file into chunks only during the encryption procedure and decryption procedure; this increases the efficiency of the parallel chunk encryption scheme.

5.6 RESULT AND DISCUSSION

Experimental tests were carried out in this section to measure performance. The proposed method is run on a Java platform with a 2 GB RAM Intel core. Encryption and decryption computing throughput are calculated. The PCE system verifies the data storage security with the help of a forward chunk approach to offer data security over a cloud network. Simulations have been carried out in this section to measure performance. In the suggested method, PCE encrypting and deciphering procedures are employed to encode and decode data of the various file (in GB). The Key generation is also done.

The security aspect of the PCE encryption approach has been enhanced. The outcome of the suggested scheme is depicted in Table 5.2. PCE's encryption and decryption times are compared to the AES [8] performance metrics, and the PCE is discovered to be superior.

Encryption Stage: The time it would take to encrypt data is referred to as the encryption period. It is also used to evaluate the performance of an encoding solution and determine the overall speed of a system or network. The encryption time is well-defined by assessing the aggregate of time it yields to produce ciphertext from plaintext, and this is shown visually in the following figure 5.4.

Decryption Stage: The decryption progression is the opposite of the encryption procedure and is referred to as such. On the other hand, decryption time is defined as the amount of time it takes a decryption method to produce a plaintext from a ciphertext, as depicted in figure 5.5.

Throughput: The throughput of an encryption system is calculated as the proportion of the encrypted data file to the encryption time. The estimated throughput PCE scheme is high and plotted in Table 5.2.

$$Throughput = \frac{File\ size(GB)}{Encryption\ time}$$

Table 5.2 Empirical outcomes of the execution duration of encryption/decryption, throughput for PCE

Input Data	File Size (GB)	Encryption Time (Sec)	Decryption Time (Sec)	Throughput
I_1	1	118	113	0.00847
I2	2	230	221	0.00869
I3	3	341	598	0.00874
I4	4	458	624	0.00892

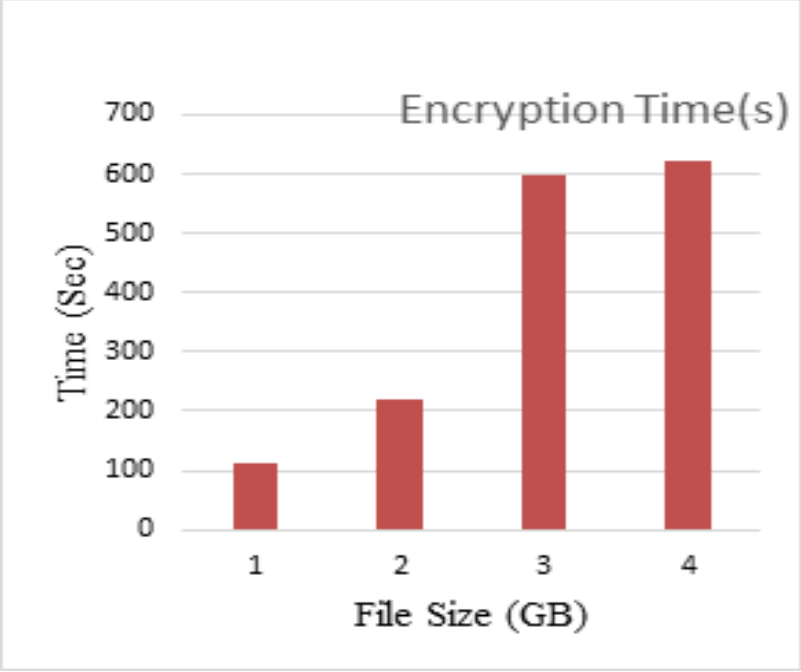

Figure 5.4 Computation time of Parallel Chunk Encryption time

The results demonstrate that the suggested solution is precise and accurate in confidentiality and accuracy and outperforms the standard AES approach that employs data confidentiality in public cloud storage.

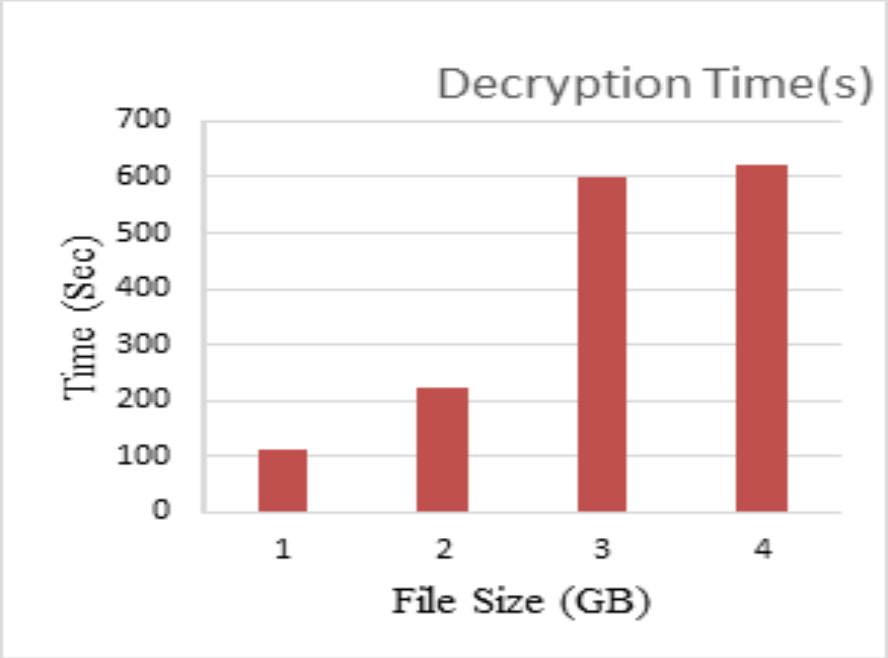

Figure 5.5 Computation time of PCE chunk decryption time

5.7 SUMMARY

Cloud services currently use many organizations to capture a large segment of today's competitive market and security issues among cloud services. The most potent service is to store info in the cloud. Cloud technology seems to be data safety in terms of confidentiality and integrity. As self-addressed in our analysis of recent research, many organizations and individuals, on-demand outsourcing their data using public cloud storage with Trusted Thirty Party Audit (TTPA) with the help of Cloud Service Provider (CSP), but the security for cloud storage, vital challenges to service providers and users. The proposed security algorithm produces an encrypted chunk with the help of the forward encipher technique. The observation result and outcome are in Table 2, and the outcome is plotted in the graph.

A comprehensive set of experimental studies is conducted to demonstrate the enhanced results associated with the proposed PCE system. The experimental results indicated that the PCE technique outperformed contemporary state-of-the-art methods. The future work scope may include scalable, quality-based encryption and mortgage information exchange with re-encryption. These are areas where we may explore the possibility of using a variety of ways for information exchange.

CHAPTER 6

CONCLUSION AND FUTURE SCOPE

6.1 CONCLUSION

The main objective of the thesis focused on reducing the risk and optimize the safety of public cloud. When companies store data physically, a lot of equipment has to be acquired, and a lot of space is needed, and it takes more time and cost to manage it. It concludes that today's worldwide cloud computing is rapidly expanding in the cloud sector. Companies and organizations need to store their vast data at a cheap cost. But we cannot sacrifice security since nobody wants someone else to access or abuse their data. Data storage in the public cloud is more beneficial than conventional storage because of its availability, scalability, performance, portability, and functional needs. Data centers and cloud service providers have provided a certain degree of client security to safeguard their company and corporate data, even though additional protection is needed for client data in public cloud storage in the areas of confidentiality, integrity, and privacy. The third chapter discusses the risks and challenges that an organization may encounter while outsourcing data to a public cloud.

For secure storing and sharing information over the public cloud, efficient encryption algorithm needs to be implemented in an energy-efficient way. The fourth chapter of the dissertation offers a unique encryption algorithm called Monarchy Butterfly Optimization ABE, which is inspired by the movement of monarch butterflies and is utilized in this chapter. A Monarchy Butterfly Optimization -Attribute Based Encryption (MBO-ABE) technique is proposed to boost the ABE technique's security outcomes in which data is encrypted and decrypted based on user attributes. The proposed MBO-ABE provides privacy for individual users when they locate the info from a public cloud. Data privacy is maintained in the public cloud by providing a unique key called a blind token for each user belonging to a specific data owner. This paper investigates the user key generation time (UKGT), and the secret key (SCSK) storage cost of the provided MBO-ABE method under various weighted characteristics.

Experimental results demonstrated that the MBO-ABE methodology exceed the existing approaches in public cloud storage, with the MBO-ABE technique achieving the highest possible performance. According to a recent study, many companies and individuals utilize public cloud storage with Trusted Thirty Party Audit (TTPA) and a Cloud Service Provider (CSP) to outsource their data on-demand. However, cloud storage security poses significant difficulties for both service providers and consumers. To make TTPA and CSP, a trusted service provider in chapter five of the thesis, proposes Parallel Chunk Encryption (PCE), a security algorithm that produces an encrypted chunk with the help of the forward encipher technique. The observation results and outcomes are analyzed based on the encryption time, and the PCE method gives users confidence that TTPA's encryption and public cloud data storage are both secure and efficient.

6.2 FUTURE SCOPE

The need for cloud computing security has skyrocketed recently. As a result, existing security measures need the inclusion of new capabilities throughout the whole cloud infrastructure. The proposed MBO-ABE technique based on Attribute-Based Encryption may be extended in the future, with lightweight authentication and block technology to improve public cloud storage systems' security. Another potential development would be to decrease the computational cost of the algorithmic formulation.

LIST OF PUBLICATIONS

LIST OF JOURNALS:

1. Nagarajan, G., & Kumar, K.S., (2021). Optimization of Security in Public Cloud Storage Using Parallel Chunk Encryption Scheme, Design Engineering (Toronto), Rogers Media Publishing Ltd, 2021(9), pp.2679-2691. (Scopus)
2. Nagarajan, G., & Kumar, K.S., (2021). A Novel Monarch Butterfly Optimization with Attribute based Encryption for Secure Public Cloud Storage. Indian Journal of Computer Science and Engineering, Eng. Journals Publications, 12(4), pp. 1044-1054. (Scopus)
3. Nagarajan, G. (2021). Comparative Analysis of Public Cloud Security Based Schemes and Cryptographic Algorithms. Turkish Journal of Computer and Mathematics Education (TURCOMAT), Karadeniz Technical University, 12(13), pg. 2114-2127. (Scopus)
4. Nagarajan, G., & Kumar, K.S., (2019). A Security Risk on Data Storage in Cloud based System–Survey. International Journal on Emerging Technologies, Research Trend, 10(2), pp.195-199. (Scopus)

LIST OF CONFERENCES:

1. Nagarajan, G., & Kumar, K. S. (2021, March). Security Threats and Challenges in Public Cloud Storage. In 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) (pp. 97-100). IEEE. (Scopus Indexed)
2. Nagarajan, G., & Kumar, K.S. (2021, March). Comparative Analysis of Public Cloud Security Based Schemes and Cryptographic Algorithms. International Conference on Intelligent Computing Smart Communication and Network Technologies (ICICSCNT 2021) held at R.M.K Engineering College.
3. Nagarajan, G., & Kumar, K.S. (2020, March). Secured Virtualized Cloud Data Storage Using Parallel Chunk Encryption with Forward Encipher Technique. International Conference on Mathematical Sciences (ICMS -2020), Sathyabama Institute of Science and Technology Chennai.

REFERENCES

[1] V. Kundra, “Federal cloud computing strategy,” *Fed. Cloud Comput. Strateg. Considerations*, pp. 1–37, 2012.

[2] P. Mell and T. Grance, “The NIST-National Institute of Standars and Technology- Definition of Cloud Computing,” *NIST Spec. Publ. 800-145*, p. 7, 2011.

[3] M. Jadhwani, P., Mackinnon, J. and Elrefal, “Cloud Computing Building a Framework for Successful Transition,” *White Pap. GTSI Corp.*, vol. 2, no. 9, 2009.

[4] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, “A break in the clouds,” *ACM SIGCOMM Comput. Commun. Rev.*, vol. 39, no. 1, pp. 50–55, 2008, doi: 10.1145/1496091.1496100.

[5] B. Furht and A. Escalante, *Handbook of Cloud*. 2010.

[6] S. K. Sood, “A combined approach to ensure data security in cloud computing,” *J. Netw. Comput. Appl.*, vol. 35, no. 6, pp. 1831–1838, 2012, doi: 10.1016/j.jnca.2012.07.007.

[7] D. I. George Amalarethinam and B. Fathima Mary, “Data Security Enhancement in Public Cloud Storage Using Data Obfuscation and Steganography,” *Proc. - 2nd World Congr. Comput. Commun. Technol. WCCCT 2017*, no. June 2018, pp. 181–184, 2017, doi: 10.1109/WCCCT.2016.52.

[8] L. Arockiam, S. Monikandan, and P. D. Sheba K Malarchelvi, “Obfuscrypt: A Novel Confidentiality Technique for Cloud Storage,” *Int. J. Comput. Appl.*, vol. 88, no. 1, pp. 17–21, 2014, doi: 10.5120/15315-3613.

[9] C. T. Huang *et al.*, “Survey on securing data storage in the cloud,” *APSIPA Trans. Signal Inf. Process.*, vol. 3, no. 2014, 2014, doi: 10.1017/ATSIP.2014.6.

[10] I. KMeenakshi and V. Sudha George, “Cloud Server Storage Security Using TPA,” *Int. J. Adv. Res. Comput. Sci. Technol. Issue Spec.*, vol. 2, no. March, pp. 295–299, 2014, [Online]. Available: www.ijarcst.com.

[11] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, “Privacy-preserving public auditing for secure cloud storage,” *IEEE Trans. Comput.*, vol. 62, no. 2, pp. 362–375, 2013, doi: 10.1109/TC.2011.245.

[12] A. Majdzadeh, Z. Wu, H. Lui, D. I. McLean, and H. Zeng, “Investigation of optically cleared human skin in combined multiphoton and reflectance confocal microscopy,”*Nov. Tech. Microsc. NTM 2015*, 2015, doi: 10.1364/ntm.2015.nm4c.6.

[13] NIST, “NIST Cloud Computing Reference Architecture: Recommendations of NIST,” *Natl. Inst. Stand. Technol.*, vol. Special Pu, pp. 1–35, 2011, [Online]. Available:https://pmteu.hosted.exlibrisgroup.com/permalink/f/gvehrt/TN_cdi_ieee_primary_6012797.

[14] C. Onwubiko, “Security Issues to Cloud Computing,” pp. 271–288, 2010, doi: 10.1007/978-1-84996-241-4_16.

[15] M. Armbrust *et al.*, “A view of cloud computing,” *Commun. ACM*, vol. 53, no. 4, pp. 50–58, 2010, doi: 10.1145/1721654.1721672.

[16] C. Mukundha Associate Professor and K. Vidyamadhuri, “Cloud Computing Models : A Survey,” vol. 10, no. 5, pp. 747–761, 2017, [Online]. Available: http://www.ripublication.com.

[17] Y. H. Wang and I. C. Wu, “Achieving high and consistent rendering performance of java AWT/Swing on multiple platforms,” *Softw. - Pract. Exp.*, vol. 39, no. 7, pp. 701–736, 2009, doi: 10.1002/spe.

[18] J. Ju, J. Wu, J. Fu, and Z. Lin, “A survey on cloud storage,” *J. Comput.*, vol. 6, no. 8, pp. 1764–1771, 2011, doi: 10.4304/jcp.6.8.1764-1771.

[19] Microsoft Azure, “Public Cloud vs Private Cloud vs Hybrid Cloud.” https://azure.microsoft.com/en-us/overview/what-are-private-public-hybrid-clouds/#deployment-options.

[20] “cybersecurity-insiders-2019-cloud-security-report,2019.” .

[21] “Emerging Public Cloud Security Challenges in 2020.” https://cloudcheckr.com/cloud-compliance/emerging-public-cloud-security-challenges/ (accessed Sep. 24, 2021).

[22] R. Kirubakaramoorthi, D. Arivazhagan, and D. Helen, “Survey on encryption techniques used to secure cloud storage system,” *Indian J. Sci. Technol.*, vol. 8, no. 36, pp. 1–7, 2015, doi: 10.17485/ijst/2015/v8i36/87861.

[23] G. Jain and V. Sejwar, “Improving the security by using various cryptographic techniques in cloud computing,” *Proc. 2017 Int. Conf. Intell. Comput. Control Syst. ICICCS 2017*, vol. 2018-Janua, pp. 23–28, 2017, doi: 10.1109/ICCONS.2017.8250721.

[24] R. Nigoti, M. Jhuria, and S. Singh, “International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS) A Survey of Cryptographic Algorithms for Cloud Computing,” pp. 141–146, 2013.

[25] Б. Жожи, “DES , AES and Blowfish : Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis DES , AES and Blowfish : Symmetric Key Cryptography.”

[26] G. Jain, N. and Kaur, “Implementing DES algorithm in cloud for data security,” *VSRD-IJCSIT*, vol. 2, no. 4, pp. 316–321, 2012.

[27] A. Pansotra and S. P. Singh, “Cloud security algorithms,” *Int. J. Secur. its Appl.*, vol. 9, no. 10, pp. 353–360, 2015, doi: 10.14257/ijsia.2015.9.10.32.

[28] X. Zhou and X. Tang, “Research and implementation of RSA algorithm for encryption and decryption,” *Proc. 6th Int. Forum Strateg. Technol. IFOST 2011*, vol. 2, pp. 1118–1121, 2011, doi: 10.1109/IFOST.2011.6021216.

[29] J. S. Resende, R. Martins, and L. Antunes, “Enforcing Privacy and Security in Public Cloud Storage,” *2018 16th Annu. Conf. Privacy, Secur. Trust. PST 2018*, pp. 2–6, 2018, doi: 10.1109/PST.2018.8514195.

[30] H. Graupner, K. A. Torkura, M. I. H. Sukmana, and C. Meinel, “Secure deduplication on public cloud storage,” *ACM Int. Conf. Proceeding Ser.*, pp. 34–41, 2019, doi: 10.1145/3335484.3335502.

[31] S. More and S. Chaudhari, “Third Party Public Auditing Scheme for Cloud Storage,” *Procedia Comput. Sci.*, vol. 79, pp. 69–76, 2016, doi: 10.1016/j.procs.2016.03.010.

[32] Y. Ren, J. Shen, J. Wang, J. Han, and S. Lee, “Mutual verifiable provable data auditing in public cloud storage,” *J. Internet Technol.*, vol. 16, no. 2, pp. 317–323, 2015, doi: 10.6138/JIT.2015.16.2.20140918.

[33] X. Li and R. Hao, “A note on ‘enhancing cloud storage security against a new replay attack with an efficient public auditing scheme,’” *ACM Int. Conf. Proceeding Ser.*, pp. 48–51, 2019, doi: 10.1145/3358528.3358588.

[34] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, “Enabling public auditability and data dynamics for storage security in cloud computing,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 5, pp. 847–859, 2011, doi: 10.1109/TPDS.2010.183.

[35] Nelmiawati and W. Arifandi, “A Seamless Secret Sharing Scheme Implementation for Securing Data in Public Cloud Storage Service,” *Proc. 2018 Int. Conf. Appl. Eng. ICAE 2018*, pp. 1–5, 2018, doi: 10.1109/INCAE.2018.8579388.

[36] C. C. Erway, A. Küpç;ü, C. Papamanthou, and R. Tamassia, “Dynamic provable data possession,” *ACM Trans. Inf. Syst. Secur.*, vol. 17, no. 4, 2015, doi: 10.1145/2699909.

[37] G. Amalarethinam, “Security Enhancement for Public Cloud Storage with Minimum Cost Security Enhancement for Public Cloud Storage with Minimum Cost,” no. January 2018, 2020.

[38] A. Sidhu and R. Mahajan, “of Recent Scientific RESEARCH ARTICLE ENHANCING SECURITY IN CLOUD COMPUTING STRUCTURE BY HYBRID ENCRYPTION,” *Int. J. Recent Sci. Res.*, vol. 5, no. 1, pp. 128–132, 2014.

[39] Y. Xue, K. Xue, N. Gai, J. Hong, D. S. L. Wei, and P. Hong, “An Attribute-Based Controlled Collaborative Access Control Scheme for Public Cloud Storage,” *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 11, pp. 2927–2942, 2019, doi: 10.1109/TIFS.2019.2911166.

[40] L. Zhou, V. Varadharajan, and M. Hitchens, “Achieving secure role-based access control on encrypted data in cloud storage,” *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 12, pp. 1947–1960, 2013, doi: 10.1109/TIFS.2013.2286456.

[41] J. Yuan and S. Yu, “Secure and constant cost public cloud storage auditing with deduplication,” *2013 IEEE Conf. Commun. Netw. Secur. CNS 2013*, pp. 145–153, 2013, doi: 10.1109/CNS.2013.6682702.

[42] J. Liu, X. A. Wang, K. Zhao, and H. Wang, “Secure Public Cloud Storage Auditing with Deduplication: More Efficient and Secure,” *Lect. Notes Data Eng. Commun. Technol.*, vol. 47, pp. 290–300, 2020, doi: 10.1007/978-3-030-39746-3_31.

[43] W. Shen, J. Yu, R. Hao, and X. A. Wang, “A Public Cloud Storage Auditing Scheme with Lightweight Authenticator Generation,” *Proc. - 2015 10th Int. Conf. P2P, Parallel, Grid, Cloud Internet Comput. 3PGCIC 2015*, pp. 36–39, 2015, doi: 10.1109/3PGCIC.2015.47.

[44] Y. Zhang, H. Zhang, R. Hao, and J. Yu, “Authorized identity-based public cloud storage auditing scheme with hierarchical structure for large-scale user groups,” *China Commun.*, vol. 15, no. 11, pp. 122–137, 2018, doi: 10.1109/CC.2018.8543053.

[45] S. Arul Oli and L. Arockiam, “Confidentiality Technique to Encrypt and Obfuscate Non-Numerical and Numerical Data to Enhance Security in Public Cloud Storage,” *Proc. - 2nd World Congr. Comput. Commun. Technol. WCCCT 2017*, pp. 176–180, 2017, doi: 10.1109/WCCCT.2016.51.

[46] C. Hahn, H. Kwon, and J. Hur, “Toward Trustworthy Delegation: Verifiable Outsourced Decryption with Tamper-Resistance in Public Cloud Storage,” *IEEE Int. Conf. Cloud Comput. CLOUD*, vol. 2018-July, pp. 920–923, 2018, doi: 10.1109/CLOUD.2018.00136.

[47] X. Dong, J. Yu, Y. Luo, Y. Chen, G. Xue, and M. Li, “Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing,” *Comput. Secur.*, vol. 42, pp. 151–164, 2014, doi: 10.1016/j.cose.2013.12.002.

[48] S. Seo, M. Nabeel, and X. Ding, “An Ef fi cient Certi fi cateless Encryption for Secure Data Sharing in Public Clouds,” pp. 1–14, 2013.

[49] T. S. Fun, A. Samsudin, and Z. F. Zaaba, “Enhanced security for public cloud storage with honey encryption,” *Adv. Sci. Lett.*, vol. 23, no. 5, pp. 4232–4235, 2017, doi: 10.1166/asl.2017.8324.

[50] C. Liu, R. Ranjan, C. Yang, X. Zhang, L. Wang and J. Chen, “MuR-DPA: Top-Down Levelled Multi-Replica Merkle Hash Tree Based Secure Public Auditing for Dynamic Big Data Storage on Cloud,” *IEEE Trans. Comput.*, vol. 64, no. 9, pp. 2609–2622.

[51] R. Sugumar and S. B. S. Imam, “Symmetric encryption algorithm to secure outsourced data in public cloud storage,” *Indian J. Sci. Technol.*, vol. 8, no. 23, 2015, doi: 10.17485/ijst/2015/v8i23/79210.

[52] A. Hadi, S., Alireza, S., Behnam, B. and Mohammadraze, “Cryptanalysis of 7-Round AES-128,” *Int. J. Comput. Appl.*, vol. 10, no. 2, pp. 21–29, 2013.

[53] A. Jivanyan, R. Yeghiazaryan, A. Darbinyan, and A. Manukyan, “Secure collaboration in public cloud storages,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9334, pp. 190–197, 2015, doi: 10.1007/978-3-319-22747-4_15.

[54] W. Wang, C., Wang, Q., Ren, K. and Lou, “Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing,” *Proc. IEEE INFOCOM*, 2010.

[55] S. Cherillath Sukumaran and M. Mohammed, “DNA Cryptography for Secure Data Storage in Cloud,” *Int. J. Netw. Secur.*, vol. 20, no. 3, pp. 447–454, 2018, doi: 10.6633/IJNS.201805.20(3).06.

[56] R. A. Id, N. Z. Id, and J. Garside, *An effective , secure and efficient tagging method for integrity protection of outsourced data in a public cloud storage*. 2020.

[57] X. Yu, P. Ning, and M. A. Vouk, “Enhancing security of Hadoop in a public cloud,” *2015 6th Int. Conf. Inf. Commun. Syst. ICICS 2015*, pp. 38–43, 2015, doi: 10.1109/IACS.2015.7103198.

[58] K. Liang *et al.*, “A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing,” *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 10, pp. 1667–1680, 2014, doi: 10.1109/TIFS.2014.2346023.

[59] N. Kaaniche, A. Boudguiga, and M. Laurent, “ID based cryptography for cloud data storage,” *IEEE Int. Conf. Cloud Comput. CLOUD*, pp. 375–382, 2013, doi: 10.1109/CLOUD.2013.80.

[60] O. Arki, A. Zitouni, and A. T. E. Dib, “A multi-agent security framework for cloud data storage,” *Multiagent Grid Syst.*, vol. 14, no. 4, pp. 357–382, 2018, doi: 10.3233/MGS-180296.

[61] D. Tiwari and G. R. Gangadharan, “SecCloudSharing: Secure data sharing in public cloud using ciphertext-policy attribute-based proxy re-encryption with revocation,” *Int. J. Commun. Syst.*, vol. 31, no. 5, 2018, doi: 10.1002/dac.3494.

[62] H. Tian *et al.*, “Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage,” *IEEE Trans. Serv. Comput.*, vol. 10, no. 5, pp. 701–714, 2017, doi: 10.1109/TSC.2015.2512589.

[63] Y. Peng, W. Zhao, F. Xie, Z. H. Dai, Y. Gao, and D. Q. Chen, “Secure cloud storage based on cryptographic techniques,” *J. China Univ. Posts Telecommun.*, vol. 19, no. SUPPL. 2, pp. 182–189, 2012, doi: 10.1016/S1005-8885(11)60424-X.

[64] R. L. Contiu S., Leblond E., “Benchmarking Cryptographic Schemes for Securing Public Cloud Storages. In: Chen L., Reiser H. (eds) Distributed Applications and Interoperable Systems,” *Lect. Notes Comput. Sci.*, vol. 10320, 2017, doi: https://doi.org/10.1007/978-3-319-59665-5_12.

[65] Z. Xu, L. Wu, M. K. Khan, K. K. R. Choo, and D. He, “A secure and efficient public auditing scheme using RSA algorithm for cloud storage,” *J. Supercomput.*, vol. 73, no. 12, pp. 5285–5309, 2017, doi: 10.1007/s11227-017-2085-8.

[66] A. L, S. and Renjit J, “Implementation of Round Key AES with Honey Technique for Securing the Public Cloud Data Storage,” *Int. J. Eng. Technol.*, vol. 7, no. 3, p. 128, 2018.

[67] J. Lai, R. H. Deng, Y. Yang, and J. Weng, “Adaptable ciphertext-policy attribute-based encryption,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8365 LNCS, pp. 199–214, 2014, doi: 10.1007/978-3-319-04873-4_12.

[68] A. Irudayasamy and L. Arockiam, “Parallel Bottom-up Generalization Approach for Data Anonymization using Map Reduce for Security of Data in Public Cloud,” vol. 8, no. September, 2015, doi: 10.17485/ijst/2015/v8i.

[69] P. Vörös, D. Csubák, P. Hudoba, and A. Kiss, “Securing personal data in public cloud,” *J. Inf. Telecommun.*, vol. 4, no. 1, pp. 51–66, 2020, doi: 10.1080/24751839.2019.1686684.

[70] H. Zhong, W. Zhu, Y. Xu, and J. Cui, “Multi-authority attribute-based encryption access control scheme with policy hidden for cloud storage,” *Soft Comput.*, vol. 22, no. 1, pp. 243–251, 2018, doi: 10.1007/s00500-016-2330-8.

[71] Y. Cheng, Z. Y. Wang, J. Ma, J. J. Wu, S. Z. Mei, and J. C. Ren, “Efficient revocation in ciphertext-policy attribute-based encryption based cryptographic cloud storage,” *J. Zhejiang Univ. Sci. C*, vol. 14, no. 2, pp. 85–97, 2013, doi: 10.1631/jzus.C1200240.

[72] S. Chandel, T. Y. Ni, and G. Yang, “Enterprise cloud: Its growth & security challenges in china,” *Proc. - 5th IEEE Int. Conf. Cyber Secur. Cloud Comput. 4th IEEE Int. Conf. Edge Comput. Scalable Cloud, CSCloud/EdgeCom 2018*, pp. 144–152, 2018, doi: 10.1109/CSCloud/EdgeCom.2018.00034.

[73] S. Munir, K. and Palaniappan, “Secure Architecture for Cloud Environment,” *Cyber Secur. Threat. Concepts, Methodol. Tools, Appl. IGI Glob.*, no. 910–925, 2018.

[74] W. Nie, X. Xiao, Z. Wu, Y. Wu, F. Shen, and X. Luo, “The research of information security for the education cloud platform based on appscan technology,” *Proc. - 5th IEEE Int. Conf. Cyber Secur. Cloud Comput. 4th IEEE Int. Conf. Edge Comput. Scalable Cloud, CSCloud/EdgeCom 2018*, pp. 185–189, 2018, doi: 10.1109/CSCloud/EdgeCom.2018.00040.

[75] R. Li, C. Shen, H. He, X. Gu, Z. Xu, and C. Z. Xu, “A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing,” *IEEE Trans. Cloud Comput.*, vol. 6, no. 2, pp. 344–357, 2018, doi: 10.1109/TCC.2017.2649685.

[76] X. Zheng, R. R. Mukkamala, R. Vatrapu, and J. Ordieres-Mere, “Blockchain-based personal health data sharing system using cloud storage,” *2018 IEEE 20th Int. Conf. e-Health Networking, Appl. Serv. Heal. 2018*, 2018, doi: 10.1109/HealthCom.2018.8531125.

[77] A. Mondal, S. Paul, R. T. Goswami, and S. Nath, “Cloud computing security issues challenges: A Review,” *2020 Int. Conf. Comput. Commun. Informatics, ICCCI 2020*, pp. 20–24, 2020, doi: 10.1109/ICCCI48352.2020.9104155.

[78] S. A. Aljawarneh and M. B. Yassein, “A conceptual security framework for cloud computing issues,” *Int. J. Intell. Inf. Technol.*, vol. 12, no. 2, pp. 12–24, 2016, doi: 10.4018/IJIIT.2016040102.

[79] M. B. . Shaikh A.H., “Security Issues in Cloud Computing,” *Intell. Comput. Networking. Lect. Notes Networks Syst.*, vol. 146, 2020, doi: https://doi.org/10.1007/978-981-15-7421-4_6.

[80] and S. K. P. Singh, Vaishali, “Revisiting Cloud Security Threats: IP Spoofing,” *Soft Comput. Theor. Appl. Proc. SoCTA 2018*, p. 226, 2020.

[81] I. A. Awan, M. Shiraz, M. U. Hashmi, Q. Shaheen, R. Akhtar, and A. Ditta, “Secure Framework Enhancing AES Algorithm in Cloud Computing,” vol. 2020, 2020.

[82] G. S. Mahmood, D. J. Huang, and B. A. Jaleel, “Achieving an Effective , Confidentiality and Integrity of Data in Cloud Computing,” no. May, 2019, doi: 10.6633/IJNS.201903.

[83] O. Saeed and R. A. Shaikh, “A User-Based Trust Model for Cloud Computing Environment,” vol. 9, no. 3, pp. 337–346, 2018.

[84] K. V Pradeep, V. Vijayakumar, and V. Subramaniyaswamy, “An Efficient Framework for Sharing a File in a Secure Manner Using Asymmetric Key Distribution Management in Cloud Environment,” vol. 2019, 2019.

[85] K. Kpelou, M. and Kishore, “Lightweight security framework for data outsourcing and storage in mobile cloud computing.,” *Int. J. Recent Technol. Eng.*, vol. 8, no. 2, 2019.

[86] I. A. Elgendy, W. Zhang, C. Liu, and C. Hsu, “An Efficient and Secured Framework for Mobile Cloud Computing,” vol. 7161, no. c, pp. 1–10, 2018, doi: 10.1109/TCC.2018.2847347.

[87] R. Saha, G. Geetha, G. Kumar, and T. Kim, “RK-AES : An Improved Version of AES Using a New Key Generation Process with Random Keys,” vol. 2018, 2018.

[88] S. Ghosh and V. Karar, “Blowfish hybridized weighted attribute-based encryption for secure and efficient data collaboration in cloud computing,” *Appl. Sci.*, vol. 8, no. 7, 2018, doi: 10.3390/app8071119.

[89] Y. Song and H. Wang, “Efficient Attribute-Based Encryption with Privacy-Preserving Key Generation and Its Application in Industrial Cloud,” vol. 2019, 2019.

[90] N. Systems, “Attribute-Based Encryption Optimized for Cloud Computing,” pp. 566–577, 2015.

[91] G. Wang, S. Deb, and Z. Cui, “Monarch butterfly optimization,” *Neural Comput. Appl.*, 2015, doi: 10.1007/s00521-015-1923-y.

[92] M. Alweshah *et al.*, “The monarch butterfly optimization algorithm for solving feature selection problems,” *Neural Comput. Appl.*, vol. 0, 2020, doi: 10.1007/s00521-020-05210-0.

[93] H. M. Alaidaros, M. F. A. Rasid, and A. S. K. Encryption, “Enhancing Security Performance with Parallel Crypto Operations in SSL Bulk Data Transfer Phase,” no. May, pp. 14–17, 2007.

[94] S. Annadurai, M. Ramchandran, and R. D. Jathanna, “Proceedings of First International Conference on Smart System , Innovations and Computing,” no. January, 2018, doi: 10.1007/978-981-10-5828-8.

[95] S. Ashokkumar, K. Karuppasamy, B. Srinivasan, and V. Balasubramanian, “Parallel Key Encryption for CBC and Interleaved CBC,” vol. 2, no. 1, pp. 21–25, 2010.

[96] S. R. Pujar, “Survey on Data Integrity and Verification for Cloud Storage,” 2020.

[97] “Cybersecurity Insiders 2019 Cloud Security Report.” https://www.cybersecurity-insiders.com/portfolio/2019-cloud-security-report-isc2/ (accessed Sep. 26, 2021).

[98] K. Abouelmehdi and A. Bentajer, “ScienceDirect CS-IBE : A A Data Data Confidentiality Confidentiality System System in in Public Public Cloud Cloud Storage Storage System System,” *Procedia Comput. Sci.*, vol. 141, pp. 559–564, 2018, doi: 10.1016/j.procs.2018.10.126.

[99] B. Chen, L. Wu, and K. R. Choo, “A Parallel and Forward Private Searchable Public-Key Encryption for Cloud-Based Data Sharing,” pp. 28009–28020, 2020.

[100] I. El, R. Ben, and F. Mrabti, “A secure and efficient remote data auditing scheme for cloud storage,” *J. King Saud Univ. - Comput. Inf. Sci.*, no. xxxx, 2019, doi: 10.1016/j.jksuci.2019.02.011.

[101] A. Kumar, “A Novel Privacy Preserving HMAC Algorithm Based on Homomorphic Encryption and Auditing for Cloud,” pp. 198–202, 2020.

[102] L. Yang, K. Xu, and S. Liu, “PADP : A parallel data possession audit model for cloud storage,” pp. 1–15, 2017, doi: 10.1002/cpe.4154.

[103] R. Swathi and T. Subha, “Enhancing data storage security in Cloud using Certificateless public auditing,” *Proc. 2017 2nd Int. Conf. Comput. Commun. Technol. ICCCT 2017*, pp. 348–352, 2017, doi: 10.1109/ICCCT2.2017.7972299.

[104] L. Yang and Z. Wang, “Research and design of multi dimension protection system for data security in cloud computing environment,” *Proc. - 2017 Int. Conf. Comput. Technol. Electron. Commun. ICCTEC 2017*, pp. 372–375, 2017, doi: 10.1109/ICCTEC.2017.00086.

[105] S. Wang, D. Zhang, Y. Zhang, and L. Liu, “Efficiently revocable and searchable attribute-based encryption scheme for mobile cloud storage,” *IEEE Access*, vol. 6, no. c, pp. 30444–30457, 2018, doi: 10.1109/ACCESS.2018.2846037.

[106] Z. Xu and K. M. Martin, “Dynamic user revocation and key refreshing for attribute-based encryption in cloud storage,” *Proc. 11th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. - 11th IEEE Int. Conf. Ubiquitous Comput. Commun. IUCC-2012*, pp. 844–849, 2012, doi: 10.1109/TrustCom.2012.136.

[107] N. Tirthani, “Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography.”

[108] Z. Kartit and M. El Marraki, “Applying encryption algorithm to enhance data security in cloud storage,” *Eng. Lett.*, vol. 23, no. 4, pp. 277–282, 2015.

[109] B. Lee, E. K. Dewi, and M. F. Wajdi, “Lee2018.Pdf,” pp. 4–8, 2018.

[110] A. Singh and K. Chatterjee, “Cloud security issues and challenges: A survey,” *J. Netw. Comput. Appl.*, vol. 79, pp. 88–115, 2017, doi: 10.1016/j.jnca.2016.11.027.

[111] S. Han and J. Xing, “Ensuring data storage security through a novel third party auditor scheme in cloud computing,” *CCIS2011 - Proc. 2011 IEEE Int. Conf. Cloud Comput. Intell. Syst.*,pp. 264–268, 2011, doi: 10.1109/CCIS.2011.6045072.

[112] L. Kumar and V. Rishiwal, “Design of Retrievable Data Perturbation Approach and TPA for Public Cloud Data Security,” *Wirel. Pers. Commun.*, vol. 108, no. 1, pp. 235–251, 2019, doi: 10.1007/s11277-019-06399-7.

[113] F. Lakrami, N. Elkamoun, and M. El Kamili, “Advances in Ubiquitous Networking,” *Lect. Notes Electr. Eng.*, vol. 366, pp. 287–300, 2016, doi: 10.1007/978-981-287-990-5.

[114] T. Bhatia and A. K. Verma, “Data security in mobile cloud computing paradigm: a survey, taxonomy and open research issues,” *J. Supercomput.*, vol. 73, no. 6, pp. 2558–2631, 2017, doi: 10.1007/s11227-016-1945-y.

[115] E. Mehraeen, M. Ghazisaeedi, J. Farzi, and S. Mirshekari, “Security Challenges in Healthcare Cloud Computing: A Systematic Review,” *Glob. J. Health Sci.*, vol. 9, no. 3, p. 157, 2016, doi: 10.5539/gjhs.v9n3p157.

[116] Y. Shin, D. Koo, and J. Hur, “Survey of secure data deduplication schemes for cloud storage systems,” *ACM Comput. Surv.*, vol. 49, no. 4, 2017, doi: 10.1145/3017428.

[117] K. Fan, M. Liu, G. Dong, and W. Shi, “Enhancing cloud storage security against a new replay attack with an efficient public auditing scheme,” *J. Supercomput.*, vol. 76, no. 7, pp. 4857–4883, 2020, doi: 10.1007/s11227-018-2645-6.

[118] P. Vijayakumar *et al.*, “MGPV: A novel and efficient scheme for secure data sharing among mobile users in the public cloud,” *Futur. Gener. Comput. Syst.*, vol. 95, pp. 560–569, 2019, doi: 10.1016/j.future.2019.01.034.

[119] B. Sengupta and S. Ruj, “Publicly verifiable secure cloud storage for dynamic data using secure network coding,” *ASIA CCS 2016 - Proc. 11th ACM Asia Conf. Comput. Commun. Secur.*, pp. 107–118, 2016, doi: 10.1145/2897845.2897915.

[120] J. Zhou, “On the security of cloud data storage and sharing,” *SCC 2014 - Proc. 2nd Int. Work. Secur. Cloud Comput.*, p. 1, 2014, doi: 10.1145/2600075.2600087.

[121] L. Chen and D. B. Hoang, “Novel data protection model in healthcare cloud,” *Proc.- 2011 IEEE Int. Conf. HPCC 2011 - 2011 IEEE Int. Work. FTDCS 2011 - Workshops 2011 Int. Conf. UIC 2011- Work. 2011 Int. Conf. ATC 2011*, pp. 550–555, 2011, doi: 10.1109/HPCC.2011.148.

[122] W. Huang, A. Ganjali, B. H. Kim, S. Oh, and D. Lie, “The state of public Infrastructure-as-a-Service cloud security,” *ACM Comput. Surv.*, vol. 47, no. 4, 2015, doi: 10.1145/2767181.

[123] A. Butoi and N. Tomai, “Secret sharing scheme for data confidentiality preserving in a public-private hybrid cloud storage approach,” *Proc. - 2014 IEEE/ACM 7th Int. Conf. Util. Cloud Comput. UCC 2014*, no. see IV, pp. 992–997, 2014, doi: 10.1109/UCC.2014.163.

[124] N. Thillaiarasu and S. ChenthurPandian, “A novel scheme for safeguarding confidentiality in public clouds for service users of cloud computing,” *Cluster Comput.*, vol. 22, pp. 1179–1188, 2019, doi: 10.1007/s10586-017-1178-8.

[125] C. Zhang, E. C. Chang, and R. H. C. Yap, “Tagged-mapreduce: A general framework for secure computing with mixed-sensitivity data on hybrid clouds,” *Proc. - 14th IEEE/ACM Int. Symp. Clust. Cloud, Grid Comput. CCGrid 2014*, pp. 31–40, 2014, doi: 10.1109/CCGrid.2014.96.

[126] G. Kulkarni, N. Patil, and P. Patil, “Private Cloud Secure Computing,” *Ijsce*, vol. 2, no. 1, pp. 75–77, 2012.

[127] S. Kamara and K. Lauter, “Cryptographic cloud storage,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6054 LNCS, pp. 136–149, 2010, doi: 10.1007/978-3-642-14992-4_13.

[128] R. Chen, Y. Mu, G. Yang, F. Guo, and X. Wang, “Dual-server public-key encryption with keyword Search for secure cloud storage,” *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 4, pp. 789–798, 2016, doi: 10.1109/TIFS.2015.2510822.

[129] Z. Wang and Y. Zhu, “A centralized HIDS framework for private cloud,” *Proc. - 18th IEEE/ACIS Int. Conf. Softw. Eng. Artif. Intell. Netw. Parallel/Distributed Comput. SNPD 2017*, pp. 115–120, 2017, doi: 10.1109/SNPD.2017.8022709.

[130] S. S. M. Chow, C. K. Chu, X. Huang, J. Zhou, and R. H. Deng, “Dynamic secure cloud storage with provenance,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6805 LNCS, pp. 442–464, 2012, doi: 10.1007/978-3-642-28368-0_28.

[131] C. Wang, K. Ren, W. Lou, and J. Li, “Toward publicly auditable secure cloud data storage services,” *IEEE Netw.*, vol. 24, no. 4, pp. 19–24, 2010, doi: 10.1109/MNET.2010.5510914.

[132] B. Lavanya and V. Thamizhthendral, “A novel data ciphering method for secure cloud storage,” *Proc. - Int. Carnahan Conf. Secur. Technol.*, vol. 2019-Octob, pp. 1–6, 2019, doi: 10.1109/CCST.2019.8888439.

[133] M. Marwan, A. Kartit, and H. Ouahmane, “Security enhancement in healthcare cloud using machine learning,” *Procedia Comput. Sci.*, vol. 127, pp. 388–397, 2018, doi: 10.1016/j.procs.2018.01.136.

[134] F. Farokhi, I. Shames, and N. Batterham, “Secure and Private Cloud-Based Control Using Semi-Homomorphic Encryption,” *IFAC-PapersOnLine*, vol. 49, no. 22, pp. 163–168, 2016, doi: 10.1016/j.ifacol.2016.10.390.

[135] H. Mahmoud *et al.*, “Novel technique for steganography in fingerprints images: Design and implementation,” *2010 6th Int. Conf. Inf. Assur. Secur. IAS 2010*, pp. 48–51, 2010, doi: 10.1109/ISIAS.2010.5604078.

[136] A. El Bouchti, S. Bahsani, and T. Nahhal, “Encryption as a service for data healthcare cloud security,” *5th Int. Conf. Futur. Gener. Commun. Technol. FGCT 2016*, pp. 48–54, 2016, doi: 10.1109/FGCT.2016.7605072.

[137] L. Adhianto *et al.*, “HPCTOOLKIT: Tools for performance analysis of optimized parallel programs,” *Concurr. Comput. Pract. Exp.*, vol. 22, no. 6, pp. 685–701, 2010, doi: 10.1002/cpe.

[138] R. N. Dasari, Y. Prasanth, and O. Nagaraju, “A novel framework for cloud storage security using two way verification,” *Int. J. Appl. Eng. Res.*, vol. 12, no. 22, pp. 11787–11795, 2017.

[139] L. Cheng, Z. Jin, O. Wen, and H. Zhang, “A novel privacy preserving keyword searching for cloud storage,” *2013 11th Annu. Conf. Privacy, Secur. Trust. PST 2013*, pp. 77–81, 2013, doi: 10.1109/PST.2013.6596039.

[140] H. Tang, J. Wu, Y. Cui, J. Weng, C. Guan, and K. Ren, “Enabling ciphertext deduplication for secure cloud storage and access control,” *ASIA CCS 2016 - Proc. 11th ACM Asia Conf. Comput. Commun. Secur.*, pp. 59–70, 2016, doi: 10.1145/2897845.2897846.

[141] Y. Zhu, R. Xu, and T. Takagi, “Secure k-NN computation on encrypted cloud data without sharing key with query users,” *Cloud Comput. 2013 - Proc. 2013 Int. Work. Secur. Cloud Comput.*, pp. 55–60, 2013, doi: 10.1145/2484402.2484415.

[142] Y. Liu, S. Xiao, H. Wang, and X. A. Wang, “New provable data transfer from provable data possession and deletion for secure cloud storage,” *Int. J. Distrib. Sens. Networks*, vol. 15, no. 4, 2019, doi: 10.1177/1550147719842493.

[143] T. A. Mohanaprakash and J. Andrews, “Novel privacy preserving system for cloud data security using signature hashing algorithm,” *Proc. - Int. Carnahan Conf. Secur. Technol.*, vol. 2019-October, 2019, doi: 10.1109/CCST.2019.8888420.