Thr Al-Qaisi

A COMPARATIVE STUDY OF PRIVACY-PRESERVING TECHNIQUES FOR THE CLOUD STORAGE

THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
ATILIM UNIVERSITY

THR AL-QAISI

A MASTER'S THESIS

IN

THE DEPARTMENT OF SOFTWARE ENGINEERING

NOVEMBER 2020

ATILIM UNIVERSITY 2020

A COMPARATIVE STUDY OF PRIVACY-PRESERVING TECHNIQUES FOR THE CLOUD STORAGE

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
ATILIM UNIVERSITY

BY

THR AL-QAISI

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR

THE DEGREE OF MASTER

IN

THE DEPARTMENT OF SOFTWARE ENGINEERING

NOVEMBER 2020

Approval of the Graduate School of Natural and Applied Sciences, Atilim University.

_____

Prof. Dr. Ali Kara
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science in Software Engineering.

_____

Prof. Dr. Ali Yazıcı
Head of Department

This is to certify that we have read the thesis "A COMPARATIVE STUDY OF PRIVACY-PRESERVING TECHNIQUES FOR THE CLOUD STORAGE" submitted by Thr Satar Jabar and that in our opinion, it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

_____

Prof. Dr. Alok Mishra
Supervisor

Examining Committee Members:

Assoc. Prof. Dr. Murat Ozbayoğlu
Mathematics Department, TOBB University _____

Prof. Dr. Alok Mishra
Software Eng. Department, Atilim University _____

Asst. Prof. Dr. Gonca Gokce Menekse Dalveren
Software Eng. Department, Atilim University _____

Date: 16/November/2020

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: Thr Satar Jabar

Signature:

ABSTRACT

A COMPARATIVE STUDY OF PRIVACY-PRESERVING TECHNIQUES FOR THE CLOUD STORAGE

Al-Qaisi, Thr

M.S., Department of Software Engineering

Supervisor: Prof. Dr. Alok Mishra

November 20, 126 pages

Information and data privacy have become critical concepts in the cloud computing industry, especially as internet users seek to use the cloud environment to store their personal and sensitive data. Many cloud service providers currently offer premium and quality-based services for their users as the first initiative for building a vast cloud community. However, security and privacy violations began to emerge and evolve in the cyber world and threaten most of its infrastructure. Fortunately, much research has been achieved to develop the proper techniques to overcome data privacy's perilous challenges and find better methodologies for protecting cloud storage contents. In this work, our study focuses on comparing several forms of privacy-preserving techniques for cloud storage. The study includes a comprehensive analysis of privacy-preserving techniques and their common attributes for the aim of designing flexible, secure, and efficient solutions for the dilemma that faces data privacy. We also present an attainable solution for privacy-preserving of the cloud storage by proposing a multi-layer encryption framework with the use of one-time password authentication technology and a multi-cloud storage structure.

Keywords: Data Privacy, Data Security, Cloud computing, Cloud storage, Comparative study, Privacy-preserving, Privacy attributes, Privacy violations, Security Attacks, Privacy schemes.

ÖZ

BULUT DEPOLAMA İÇİN GİZLİLİK KORUMA TEKNİKLERİNİN KARŞILAŞTIRMALI BİR ÇALIŞMASI

Al-Qaisi, Thr

Yüksek Lisans, Yazılım Mühendisliği Bölümü

Danışman: Prof. Dr. Alok Mishra

Kasım 2020, 126 sayfa

Bilgi ve veri gizliliği, özellikle internet kullanıcılarının kişisel ve hassas verilerini bulut ortamında depolamada, bulut bilişim endüstrisi için kritik kavramlar haline geldi. Birçok bulut hizmeti sağlayıcısı, geniş bir bulut topluluğu oluşturmada öncü girişim olarak kullanıcıları için birinci sınıf ve kaliteye dayalı hizmetler sunmaktadır. Ancak, tüm dünyada siber güvenlik ve gizlilik ihlalleri artmaya ve gelişmeye ve sonununda çoğu servis sağlayıcının altyapısı tehdit edilmeye başlanmıştır. Neyse ki, veri gizliliğinin tehlikeli zorluklarının üstesinden gelmek ve bulut depolama içeriklerini korumak ve daha iyi metodolojiler bulmaya yönelik uygun teknikler geliştirmek üzere çok sayıda araştırma yapıldığı gözlemlenmektedir. Bu çalışma, bulut depolamaya yönelik gizlilik koruma tekniklerinin çeşitli biçimlerini karşılaştırmaya odaklanmaktadır. Çalışma, veri gizliliğinin karşı karşıya olduğu ikilem için esnek, güvenli ve verimli çözümler tasarlamak amacıyla, gizliliği koruma tekniklerinin ve bunların ortak özelliklerinin kapsamlı bir analizini içermektedir. Bu çalışmada ayrıca, tek seferlik parola kimlik doğrulama teknolojisi ve çoklu bulut depolama yapısı ile çok katmanlı bir şifreleme çerçevesi önererek bulut depolamanın gizliliğini korumak için ulaşılabilir bir çözüm sunulmaktadır.

Anahtar Kelimeler: Veri Gizliliği, Veri Güvenliği, Bulut bilişim, Bulut depolama, Karşılaştırmalı çalışma, Gizliliği koruma, Gizlilik özellikleri, Gizlilik ihlalleri, Güvenlik Saldırıları, Gizlilik planları.

To my parents.

ACKNOWLEDGMENTS

I would like to express my deepest gratitude to my supervisor Prof. Dr. Alok Mishra, of the Department of Software Engineering at Atilim University, for his guidance and efforts provided along my journey.

I would also express my thanks to the head of the Software engineering department, Prof. Dr. Ali Yazıcı, for all his efforts and time.

I shall also thank the examining committee Assoc. Prof. Dr. Murat Ozbayoğlu of the Mathematics Department at TOBB University and Asst. Prof. Dr. Gonca Gokce Menekse Dalveren of the department of Software Engineering Department at Atilim University.

Finally, I pray to all mighty Allah to guide me through these difficult times and set me on the right path toward a thriving future full of luck and success

TABLE OF CONTENTS

LIST OF TABLES

TABLES

LIST OF FIGURES

FIGURES

LIST OF SYMBOLS/ABBREVIATIONS

TCG	Trust Computing Group
CSA	Cloud Security Alliance
RFC	Request for Comments
TOTP	Time-based One-Time Password
OTP	One-Time Password
ABP	Automatic Blocker Protocol
TPA	Third-Party Auditor
TTPA	Trusted Third-Party Auditor
OWASP	Open Web Application Security Project
CSP	Cloud Service Provider
ORAM	Oblivious RAM
IND-CPA	Indistinguishability under chosen-plaintext attack
IBE	Identity-Based Encryption
CTR	Counter Mode
CRT	Chinese Remainder Theorem
IOT	Internet of Things
AES	Advanced Encryption Standard
DES	Data Encryption Standard
RSA	Rivest-Shamir-Adleman
SHA	Secure Hash Algorithm
SWT	Standard Widget Toolkit
DEPSKY-CA	Dependable and Secure Storage in a cloud-of-clouds
MCDB	Multi-Cloud Dependable
LSN	Local Sequence Number
ECB	Electronic Control Book
SDB	Secure Database

CryptDB	Crypto Database
DBMS	Database Management System
HASBE	Hierarchical Attribute-Role Based Access Control
IAAS	Infrastructure as a Service
PAAS	Platform as a Service
MLES	Multi-Layer Encryption System

CHAPTER 1

INTRODUCTION

The birth of computer and informatics technologies has become the digital industry's core in the past several years because of the massive contribution of these fields in various aspects of humans' lives. Simultaneously, continuous research and development in the cloud computing sector have led to a significant and unprecedented revolution in cyberspace. Therefore, people sensed the need to outsource their confidential information somewhere safe, efficient, and economical such as the cloud environment. However, with all the exaggerations of the cloud environment's ability to store data in a reliable and secure approach; A huge concern floated on the surface that threatens personal data security and confidentiality, which is information privacy. We have known information privacy for decades as a person or organization's capability to reduce the amount of visible data by other individuals. Therefore, it limits the access to sensitive data such as personal identification information, passwords, health records, and other crucial data that might endanger people, organizations, and governments if it falls into the wrong hands. Also, computers and information technologies are not the only concern of information privacy; Human privacy is considered an essential element in human writes that touches various economic and social aspects of individuals, reflecting human beings' personality. For the past two decades, the need to implement security concepts in the digital industry has increased because of the continuous presence of unwanted and harmful materials around cyberspace. The noticeable increase in the number of potential attacks forced the researchers worldwide to adopt the means to eliminate such perils. However, when researchers realized the inevitability and severity of security risks, the spark of privacy

preservation techniques broke out to uncover novel methods for safeguarding valuable data. We can define the privacy preservation techniques as a set of models and schemes designed using mathematical or cryptographic algorithms that address critical and threatening threats against different cyber sectors and, at the same time, yields the optimum solutions to establish a reliable and safe system.

Before the cyber world's evolution, people were unprepared to overcome security challenges because of the intricate design of the menaces that rendered it troublesome to process without proper implementations. In the past, the severity and impact of security threats were not that serious as today's threats. The invention of privacy-preserving techniques created the base for all security systems that ensure the confidentiality and secrecy of private and vital data. Privacy preservation techniques may vary in style and format based on the nature of the security threat. However, it shares a common intention that is privacy-preservation assurance for the working system.

On the other hand, The technological advancement in computer networks resulted in the discovery of cloud computing services that forced the analysts and researchers to re-forge privacy preservation techniques. Therefore, significant modulation is performed over privacy preservation techniques regarding compatibility, reliability, and accountability to create a suitable security countermeasure for the harsh cloud environment. Although cloud computing services offered unrivaled features and characteristics to ease the work for users and prevent security penetrations, the reliability and effectiveness of the cloud environment hinged upon whether the community is familiar with the current era of technology or not [1].

1.1 The relevance of privacy-preserving techniques

Data and information privacy are considered one of the major concerns in the current technology era. Because data and information are the centers of everything in today's life, from personal information to a wide variety of private and high-value data

that belongs to specific entities, and it is our job to protect and hide any kind of sensitive materials that touches the essential aspects of our daily work. While Privacy-preserving solutions are unique in the structure and security characteristics, the need to implement these solutions in work grows significantly without stop [2]. Indeed, Societies realized the need to embrace privacy solutions to secure private workspace and prohibit unusual attempts to steal or compromise vital data. Because Data privacy is a pivotal aspect in the digital age and the need to implement privacy techniques is growing relentlessly since the infrastructure of computer and information technologies is getting complicated and tangled daily. Privacy protection techniques helped researchers comprehend the nature of security threats and form a suitable approach to address these challenges. At first, the use of privacy preservation techniques was at its lowest levels because the digital data concept was unclear for most of society, and the cost for the development was relatively high. However, the innovation in the security and privacy concepts created a glimpse of hope toward a better cyber world full of the means to stand against attacks that threaten a variety of technology sectors.

The increasing interest in the field of cloud computing has been increased recently because of the unique capabilities and the wide selection of services it provides. Computer users, organizations, and governments find using their devices to finish particular work is inefficient and inconvenient. They also try to invest more money and time in software and hardware to process data and complete a-certain activities. In contrast, cloud computing provides these entities with on-demand access to better resources and services without additional cost and with lesser requirements possible. L. Wang et al. said about cloud computing, *"A computing Cloud is a set of network enabled services, providing scalable, QoS guaranteed, normally personalized, inexpensive computing infrastructures on demand, which could be accessed in a simple and pervasive way"* [3]. However, cloud computing is not what everyone thinks about; it also has vulnerabilities and challenges represented by security and privacy violations. Indeed, data privacy in the cloud matters more than any other cloud aspect because outsourced data can be under extreme danger in the cloud environment as

users do not have full control over their data once they upload it to the cloud storage [4]. The utilization of cloud privacy-preserving schemes has drawn much attention in the last few years because of the current situation of cloud security and the urgent need to adopt security and privacy countermeasures. The severity of dangerous materials may vary depending on the security status of the network or the system itself. For example, an adversary may attempt to access bank accounts and tries to steal some critical and sensitive information regarding access keys and identities or corrupt bank firewalls to disable the security alarms. This type of threat is considered a severe one and may yield catastrophic consequences. Another example, an attack can occur in universities or governmental institutions; an attacker may try to access the institution's network or database and manipulate results such as student grades or election results.

1.3. Research outline

1.3.1. Research Hypotheses

In this research, we will conduct a comparative study over seven privacy-preserving schemes including Sheren et al. scheme, Yuan et al. scheme, Ganapathy et al. scheme, T. Subha et al. scheme, Yu Jin et al. scheme, Zhen Yang et al. scheme, and Liu Guoxiu et al. scheme to protect cloud storage contents from cyber-attacks. we present several hypotheses regarding this subject:

- What are the most important motivations that make individuals and organizations prioritize the privacy of information when outsourcing personal and sensitive data to the cloud environment?
- How complex should the structure of a privacy-preserving scheme be to deliver an optimal security and privacy solution?
- What is the impact of privacy/common attributes on the security and privacy aspects of the cloud environment?
- Is it possible to build mutual trust between data owners, users, and cloud service providers regarding information and data privacy?

1.3.2. Research motivations and objectives

The significance of information and data privacy in today's life drives us to adopt this research type. Research is conducted in this field to help individuals and organizations analyze security and privacy requirements before designing security and privacy systems for the cloud environment to prevent any potential threats that jeopardize the user's content. Also, the primary focus here is to understand the real-time workflow of privacy schemes to create a better understanding of the privacy systems that can help in the design of novel, reliable, and enhanced models.

While The main goal of this research is to review, analyze, and conduct a comparative study on multiple privacy-preserving techniques explicitly designed to protect cloud storage contents. This research aims to find the best privacy-preserving form to use in future systems to protect the data files transmitted or stored in the cloud storage. Also, one of the essential objectives is to provide the ability for field researchers to design flexible and reliable privacy schemes by revealing the strengths and weaknesses of the existing schemes, which can give guidance for developing appropriate tools [5]. After gathering comparison results, we aim to propose a privacy-preserving framework that uses all the advantages of the compared schemes to enhance data privacy characteristics in the cloud environment.

1.3.3. Research methodology

Research methodology referred to the procedure in which researchers used to gather information and data sources regarding their field of interest. Research methods present all the capabilities of collecting and organizing data for the intended area of study [6]. This research used the literature study methodology to collect data and information from journals, articles, books, and theses, containing the required materials to conduct the study. Literature study methodology consists of three types of study techniques, including explanatory study, descriptive study, and exploratory study. Explanatory research handles two kinds of problems, a specific theme with

limited or complex sources and the other situation where researchers might not examine the issue adequately. Therefore, the explanatory research aims to create a better understanding of the problem that exists, but it does not present an inclusive solution to the problem itself.

On the other hand, exploratory research deals with the type of problem that has not been conducted or implemented for a study. Lastly, descriptive research intends to illustrate and explain the nature of the problem that needs to be studied. Our study combines two research methods (Explanatory and Descriptive) to conduct a comparison study over privacy-preserving schemes. These methodologies helped us in our search for the best route to enter this type of research, while at the same time have had a significant influence on the outcomes of the study.

1.4. The Significance of the study

The study in the thesis will provide an inclusive analysis of privacy-preserving schemes that protect cloud storage contents. The implementation of various types of privacy-preserving schemes has been conducted based on the divergence in design structure, functionality, security characteristics, and general outcomes, which will impact the understanding of the privacy preservation concept for different types of field researchers. The comparative analysis of privacy-preserving schemes provides future researchers with the capabilities and experience to design enhanced versions of privacy schemes. The selection of the privacy-preserving schemes has been conducted based on several factors, including the use of current technology, the challenges that face the security and privacy layers of cloud storage, level of complexity, and time consumption. Also, the selection of common privacy attributes relies heavily on the amount of relationship and the similar characteristics founded between privacy-preserving schemes. The thesis will also present the comparison results of privacy-preserving schemes to complete the full picture of each scheme and to gives the proper tools and enhancements for future researchers to use about the same subject. The comparative table results will present an evaluation criterion to construct the strengths

and limitations table, which will be the comparison's final results. Finally, a novel multi-layer encryption framework with one-time password technology and a multi-storage structure will be proposed based on two main factors: the data gathered from the comparative study and the design principles of privacy-preserving approaches that secure cloud storage in the cloud environment.

The thesis structure will contain the following:

Chapter one presents an entry into the world of privacy preservation and its influence on various current technology.

Chapter two introduces the idea behind privacy-preserving techniques and the recent studies involved in this subject.

Chapter three presents a comprehensive description of privacy attributes and their relevance.

Chapter four presents the comparative study of privacy-preserving schemes for cloud storage security and the methodology behind selecting both the privacy-preserving schemes and the common privacy attributes.

Chapter five discusses the outcomes of privacy-preserving schemes based on the evaluation of privacy attributes, and it also contains the review of major attributes that have not been previously addressed in other studies.

Chapter six introduces a brief look at the design principles of privacy-preserving methods and a proposition of the novel privacy-preserving framework for cloud storage.

Chapter seven concludes the study by presenting how much this study will contribute to the design of future security and privacy frameworks by summarizing the outcomes and limitations of this study.

CHAPTER 2

LITERATURE REVIEW

During the last decade, industry specialists were eager to discover useful and reliable solutions to address security challenges. Therefore, the criticality and sensitivity of security and privacy drive field researchers to develop the means to provide privacy assurance property to their work. In our turn, we dedicate the work in this chapter to unveil and demonstrate the literature done for the past decade on privacy-preserving techniques. At first, we will touch upon the concept of privacy-preserving techniques and the developments in this area. Next, we will shed light on the literature done in terms of the classification of privacy-preserving techniques. Lastly, we will classify privacy-preserving techniques according to our perspective and based on the importance and crucial nature of security events. In addition, a literature survey has been conducted on a variety of novel privacy-preserving techniques that address data and information privacy concerns.

2.1. Understanding the principle of privacy-preserving techniques

Over the past years, security measures started to emerge in the cyber world due to the rapid development in the internet and informatics fields. Therefore, field experts started to widen knowledge and awareness about the remedy of security and privacy difficulties. The first initiative started with the understanding of data preservation and the aim to seek the proper definition for privacy-preserving technique. However, researchers and security expertise analogously defined data preservation. Kumar et al. define preservation as the method of concealing the outcome of data mining operations throw the utilization of special data hiding techniques [7]. Likewise, R. Mendes

described privacy-preserving techniques for data mining "*Privacy-Preserving Data Mining (PPDM) techniques have been developed to allow for the extraction of knowledge from large datasets while preventing the disclosure of sensitive information."* [8]. Although the definitions described how privacy-preserving works in data mining, the same characteristics can be applied to different domains such as cloud computing, cybersecurity, and data analytics. Besides, the design of the privacy-preserving technique requires a unique scheme that contains essential elements with the ability of user interaction and a security violation assessment engine. JeurNagaraj, S et al. suggest an ideal architecture for a privacy-preserving technique that consists of four components, including user interface, user engine, rule engine, and cloud database [9]. Also, Pixelated (an email client project) developer Anike, A. implied the design of the privacy-preserving architecture for the email system. The architecture consists of the pixelated client, which is the user interface designed using a programming language for web applications and an email election engine. This design layout offers the possibility to establish a connection with the server from the user site, which keeps users' data in a safe environment [10].

2.2. The taxonomy of privacy-preserving techniques for the cloud storage

The ongoing evolution of cloud computing and its ability to deliver the various types of on-demand services have had an effective impact on the world of the internet and informatics fields. Cloud computing becomes the foundation stone for future developments, especially in the educational fields, which is the most vital aspect of humans' lives [11]. However, data security and privacy concerns arise and adapt over time to threaten cloud services with many variations that target sensitive information. For this reason, researchers around the world tried for the past decade to develop security and privacy countermeasures to eliminate such perils. Initially, researchers designed various frameworks and schemes without considering the importance of classification of the privacy-preserving techniques based on threat type. So, few researchers introduced survey papers around the classification of privacy-preserving techniques that targets the security of cloud storage. The study done by researchers in

[12], [14], [15], [19] took a similar classification approach. The main techniques used in each classification were access control techniques, encryption techniques, and auditing techniques. However, the huge similarity in the classification approach lies in the number and the nature of the techniques used in each study. The study in [12] took two additional techniques for privacy-preserving of cloud storage called integrity checking and keyword search. The integrity checking technique aims to verify the level of purity of the incoming and outgoing data and compare it with an earlier version of the same data to create proof of validation. While keyword search technique involves converting the plaintext form to an encrypted document and offer the ability to search the entire document for the desired keyword or full text [13]. This technique offers a unique solution to encrypt the original data before outsourcing it to the cloud environment. The study in [14] focused on conventional techniques (Access control, Encryption, and Auditability) without the mention of additional and more advanced techniques. While a study done by Liu, Y, and fellow researchers in [15] took an extra step towards developing and adopting novel techniques that can protect data privacy in the cloud. One of the newly added approaches is the isolation of users' data and cloud activities. This technique can ensure the prevention of trespassing on users' data in a multi-tenancy cloud environment. The second approach added is Trust, building mutual trust between parties is an important aspect of ensuring that each party will perform its assigned task in an organized and error-free manner [16]. On the other hand, the hardware trust techniques have also been implemented to support the soft-trust techniques in preserving the cloud's data security. Recently, TCG (Trust Computing Group, an organization for developing secure industrial standards) worked on a fresh scheme that strengthens the security and privacy in the manufactured hardware, which leads to an increase in the level of trust and reliability [17]. Finally, governance is also adopted as a critical security framework that involves creating a set of rules and regulations that control various activities in the cloud environment to overcome potential threats [18].

In the last few years, many organizations resorted to cloud computing solutions due to the continuous growth in data sizes and personal resources' limited capabilities. People involved saw a wide future in cloud computing services and its potentials to deliver a unique environment that provides cost-effective, flexible, and on-demand services. However, security and privacy concerns began to overthrow organizations' ambition to introduce a safe and reliable sphere for individuals to manage and process their data. Therefore, researchers in the field of cloud security and privacy countermeasures improve and expand their vision to introduce effective and secure privacy-preserving techniques. The study conducted in [19] inserted new methodologies to categorize privacy-preserving techniques. Singh, N & Singh, A. K. used four categories to classify privacy-preserving techniques (Cryptography, Probability, Anonymization, and Ranking). The cryptography techniques are being something complementary in every privacy-preserving scheme. Most of the researchers use encryption techniques to design schemes and models that prevent forgery and modification of the original data. The second technique involves using probability to construct schemes in a unique form that results in a predictable outcome [20]. Many researchers use this approach to render data leakage threat a solvable matter. The third technique used is data anonymization, which is the act of encrypting users 'data in a way that does not reveal the data owner's identification information. As a result, protecting the identity of the original user and provide invulnerability to identity theft attacks [21]. The last technique adopted in this research is the ranking search. Ranking search according to the [22] "*Given a query q and a collection D of documents that match the query, the problem is to rank, that is, sort, the documents in D according to some criterion so that the "best" results appear early in the result list displayed to the user*." It means that a special ranking algorithm will be implemented over a set of data in a way that preserves data security and tries to accomplish the most accurate results.

Furthermore, the research paper [23] devoted to integrating new elements in the taxonomy of privacy-preserving techniques. The remote data integrity checking protocol is one of the new technologies that provide a verification tool to substantiate

data integrity upon retrieval from cloud storage service [24]. Another technique called dynamic metadata reconstruction has been added by researchers to expand the level of diversity in the classification. The dynamic metadata reconstruction is a framework proposed in [25] to sort the metadata in the cloud storage database effectually and securely. According to the results, the proposed framework achieved a reasonable security level by limiting the ability of an adversary to expose users' privacy.

Recently, an article [26] discussed the importance of cloud security requirements and the classification of security and privacy countermeasures to protect data confidentiality. The researchers followed the guidelines of CSA (Cloud Security Alliance) [27] in the categorization of preventative measures. CSA has considered 12 different types of security-as-a-service that focuses on protecting cloud infrastructure. The categorization covers almost every domain in the cloud computing sectors, such as web applications, network communication, data storage security, physical and hardware security, and access management techniques.

2.3. Privacy-preserving techniques for cloud storage

2.3.1. Sheren et al. privacy-preserving scheme based on the one-time password and security protocol to secure cloud storage

Security researchers introduce access control approaches as the first security and privacy technique that restricts certain activities on private data to prevent distinctive types of violations in terms of privacy-preserving. Access control solutions provide an innovative method to address various security and privacy threats such as message modification, unauthorized access, masquerade, and many more forms of cyber threats against different cyber world environments. The advancement in internet security and privacy preservation forced field researchers to design such schemes to improve cloud security control and import additional security layers. Fortunately, Sheren et al. proposed a privacy-preserving scheme [28] Based on a new technology called the one-time password to prohibit untrusted access to cloud storage contents and

potential data theft of vital cloud data. Also, Sheren et al. scheme presents a familiar tool that functions as an authentication and verification mechanism to check the level of authenticity and integrity of cloud users. Sheren et al. also implemented the third-party auditor, a trusted authority used to discover corrupted data and unauthorized access to cloud storage. In addition, the scheme adds a peculiar security protocol called Automatic blocker protocol that is used as an authentication tool to assess the honesty of the third-party auditor, which might get corrupted because of its interest in critical and sensitive data belonging to cloud clients. The access control-based scheme showed promising results in terms of security and privacy performance and the effectiveness of the methodologies used.

- **Design features and workflow**
  - **One-time password technique**

As we mentioned earlier, Sheren et al. utilized an authentication tool to control access to vital cloud data. The one-time password technique uses a special standard called RFC (6238) [29], designed for access control and multiple authentication factors. The TOTP-standard structure considers two essential elements the timestamp and the secret key shared through a secure channel between cloud parties. A cryptographic hash function [30] is used to merge both elements to create the one-time password and store this password at the cloud server site until a retrieve request is received from cloud clients. Each cloud user receives the OTP through a special mobile application, where users will have the access capabilities to cloud data.

  - **Automatic blocker protocol**

For many years, the third-party auditor has been used in a variety of security and privacy-preserving scheme as an inspection tool to check the identity of cloud users and to avert any data manipulation means. However, a concern arises regarding whether a third-party auditor is a trustworthy party in the network or not. So, Sheren et al. imported another authentication tool called

ABP to check the third-party auditor's authenticity. The automatic blocker protocol mentioned in [31] consists of unique software that can inspect and evaluate requests established by different types of users (cloud users or adversaries). The application responds to the user with authorization to access if it found any compatible and similar results with cloud database, else the software will block any communication with the user and deny his access to the cloud data.

- **The OTP-based scheme's workflow**

The scheme begins functioning from the system admin side. System admin uses a special key-generation algorithm [32], [33] to create the required keys for cryptographic operations. Later, the generated keys are sent with the initialization data to the cloud service provider. Cloud service provider initializes a safe connection with system admin by replying with a message signed using a special signature generation algorithm. However, all the messages sent between the cloud service provider and system admin are encrypted with the advanced encryption standard technique. Also, clients need to register into the system to create an authentication level between clients and the system and ensure data security. The third-party auditor also needs to register into the system so that the system admin can resort to the TPA for inspection and auditing operation regarding outsourced data. When TPA registers in the system as an eligible party, he can obtain the secret key and additional information regarding the auditing process.

At this stage, TPA can send an auditing request to the cloud service provider only if the system admin issues an auditing operation over outsourced data. In the meantime, the cloud service provider asks the system admin about the third-party auditor's authenticity by requesting the results of applying the automatic blocker protocol over TPA. If the protocol returns positive results, TPA can establish the auditing process over outsourced data in the cloud storage. When

TPA finishes the auditing process, he sends an auditing report to the system admin to inform him about the auditing results and to end the connection tunnel opened between the two parties.

- **Scheme implementation and performance analysis**
  - **Test environment**

The OTP-based scheme conducts Java enterprise edition web application as the programming language to design the scheme. In addition, a Tomcat cloud server [34] has been used as a cloud server to create a cloud environment for the implementation process. Also, Sheren et al. mention a way that can preserve data confidentiality. The OTP-based scheme uses an AES cryptographic technique (Advanced Encryption Standard) to cipher all the data before outsourcing to the cloud server.

  - **Security evaluation.**

In terms of performance and security evaluation, Sheren et al. apply the OTP-based scheme into penetration software called OWASP [35], [36]. OWASP is online software which can assess the different type of web applications to measure security performance and capabilities. Multiple-types of tests has been conducted over the OTP-based scheme to evaluate and assess privacy-preservation and security properties:

1. SQL injection: this test involves the evaluation of system participants.
2. Corrupted and unauthorized access: this test involves certain types of attacks on cloud users, data owners, and cloud service providers.
3. Data exposure: this test involves measuring the level of exposure each adversary can conduct to reveal vital information about certain individuals in the cloud.

4. Cross-site request forgery: this test examines whether there is a malicious request to access user identification information and use it for dangerous acts.
5. Bad Traffic: this test involves evaluating the consistency and reliability of the connection line between users/data owners and CSP.

- **Performance criteria and experimental results**
  1. **Average request/response time versus the number of requests**: The results show a significant amount of deviation in the time needed to serve 10 and 20 user requests.
  2. **Throughput**: Also, for the results of throughput (the amount of data needed to serve users requests measured in megabits), another boost in the amount of data needed to serve users' requests is noticeable as the number of requests increases.

2.3.2. Yuan et al. privacy-preserving scheme based on ORAM for secure data sharing in cloud storage

Yuan et al. proposed a privacy-preserving scheme [37] based on the technology of ORAM (Oblivious Ram), which preserves the privacy of the shared data between multiple users. This scheme provides a unique algorithm for cloud storage management called Path-ORAM (a binary tree representation of cloud storage) that improves the model's efficiency and decreases the overall communication cost. In addition, the scheme ensures the security and prevention against access pattern behavior generated through malicious users by implementing Identity-Based Signature [38] and Basic Symmetric Cryptography algorithms [39]. In the previous versions of the ORAM based models, data owners can achieve a high-efficiency level for the users who want to access the cloud storage system. Data owners must perform a shuffling operation of the storage to reach the high level of efficiency of the system, but this task is complex, time waste, and requires so much effort from a single person. Fortunately,

the new scheme offers a solution to this matter. The design of this scheme is unique in its nature because the cloud server handles the shuffling and verification processes and lifts the burden from the data owner. However, the data owner is now given the simple task of verifying only the first block of the root node located in the binary tree. Finally, the user needs to forge a proof of authenticity to present it to the cloud server to prove that there is no malicious attempt to modify the data transmitted to the server.

- **Design features and cryptographic approaches**
  - **Cryptographic schemes**

    The scheme uses three different cryptographic algorithms to create a security barrier against different types of attacks:

    1- Identity-based signature adopts four algorithms listed below: IGen(1^k): this algorithm takes a security parameter as an input and outputs master public key and master secret key.

    2- Symmetric Encryption: This method consists of three different notations. The first one is the SGen(1^k). This notation refers to the key generation algorithm.

    3- Public key encryption: This method also consists of three notations. The first notation is PGen(1^k), which refers to the key generation algorithm.
  - **Algorithm analysis**

    As we mentioned earlier, system storage has been shaped to be in the form of a binary tree. It means that data blocks are formed based on the Path-ORAM structure [40]. At the start, the binary tree storage is being created and deployed on the cloud server by the data owner, who is responsible for several operations performed on the data blocks, including reading and write operations. In addition, the data owner can give read or write permission to specific users who want to gain access to owner data.
- **Scheme design structure**

  This section will focus on key design steps regarding the aspects of storage structure, data block format, and algorithm execution.

- **Storage Structure**

The data owner requests a database with a specific size, and the server initiates the generation process of a binary tree that must have a specific height. Besides, we should mention that the root node must have a depth of 0, and the leaf node has a depth of (height of the tree – 1). Meanwhile, the data owner must keep an eye on the I/O operations because these operations may cause an increase in the amount of information stored in a single data block. Fortunately, the data owner can use temporary storage to control data overflow and ease the task without the need for any additional storage capacity. In fact, after each I/O execution, the temporary storage will not contain any data in a single client situation. Unfortunately, things are not the same in multiple user systems because the data stored in the stash is needed every time there is a read or write operation, so in this situation, we can't store the stash at every client end. Fortunately, with this situation in hand, there is a bigger problem of sharing the stash among several users. However, there is a fix for this problem by increasing the size of the storage in the root node and make it accommodate the stash.

- **Data block format**

The data block format in single-client ORAM consists of two parts: the data block and the data itself. Also, if we want to protect the data and reach a high level of privacy and security, the data block must be encrypted before deploying to the users for the purpose of secure sharing. Also, in multiple user systems, the data block must contain unique portions of information that define the access control protocol.

- **Results and performance analysis**
  - **Security achievements**

1. Authority control

The authority management is an important feature that ensures the privacy and protection of information and keeps malicious users from getting their hands-

on sensitive data. In this scheme, the use of the IND-CPA security system (Symmetric encryption scheme), as well as the Identity-based signature scheme, help control the privileges given to the user to perform specific types of system operation. So, if the user cannot decrypt a ciphertext and obtain information, it means that the user does not pose the symmetric key for cracking the ciphertext; therefore, he does not have the permission to read that specific data block or write new content to it.

2. User proof of validity and correctness

The user needs to inform the server of the data blocks shuffle and re-encryption operations. Therefore, sending proof to the server states that every block is shuffled and re-encrypted without any suspicious operation. In addition, the fresh data blocks need to be sent by the user to the data owner so he can check the validity and the correctness, therefore replacing the root node data block with the new one after getting a positive result from the verification test.

3. Concealing access patterns from server

During the read operation, the user writes an empty data block after reading the data block to achieve the goal, which is the server cannot distinguish whether the operation is read or write. With the situation at hand, we can say that the scheme uses a high-security system that can hide access patterns from the cloud server.

- **Performance analysis**

The scheme was programmed and executed using C++ and performed on Ubuntu 16.04 PC with Intel Core i5 CPU and 4GB main memory. The server uses MongoDB as the outsourced cloud database and storage [41].

- **Implementation tools**

1- Identity-based signature: the scheme uses the Stanford IBE library v0.7.2 [42] to implement an identity-based signature.

2- Symmetric Encryption: Counter (CTR) mode of the Advanced Encryption Standard (AES) is the main cryptographic technique used for encryption and decryption operations [39].

3- Public Key Encryption: the scheme also uses a secondary cryptographic technique called the Elgmal encryption algorithm, which uses BIGNUM in the OpenSSL library as a tool to execute calculations [43].

- **Experimental results**

  The scheme adopts two parameters to perform an experimental evaluation:

  - **Amortized cost**

    The amortized cost can be defined as the accumulated portion of the recorded cost of a fixed asset that has been charged to expense through either depreciation or amortization [44]. So, in this scheme, when the database size increases from 2^7 to 2^{12} blocks, each of which is 4KB in size. The amortized cost per operation will be double in the amount. However, in the situation when the storage size is equal to 0.5GB and the block size increases gradually from 1KB to 4KB. In this case, the amortized cost will slightly decrease with the increase of the block size. Finally, we can conclude that the impact of the storage size is significant on the system's performance. However, the situation is not the same in block size because the block size impact can barely affect the working system's efficiency.

  - **Unit operation efficiency**

    Yuan et al. scheme has proven to be very efficient in terms of a single unit operation read or write. The reason behind this result is that the scheme uses unique methods for encryption and decryption to manage access control problems.

2.3.3 Ganapathy, S et al. scheme based on CRT theorem that ensures storage security and privacy preservation in the cloud

Ganapathy, S et al. proposed a secure storage scheme [45] to meet cloud and IoT environments' needs in terms of securing storage and controlling access to

different types of personal and sensitive data. The uniqueness and security promises made this scheme one of the novelties schemes that address the threats of data theft and unauthorized access that may jeopardize crucial information. The secured storage scheme selects unique mechanisms for building secure storage that can preserve the privacy of its data and preventing any attempt to steal or modify crucial information. As we can obtain from the scheme's name, the famous Chinese remainder theorem [46] has been introduced to construct new algorithms for encryption/decryption, which can produce highly secure storage. Also, the CRT has been used to design a new key generation algorithm that can generate complex and secure keys. Besides, A key management system for securing and managing encryption/decryption keys is implemented. The key management system allows the system administrator or the file owner to build an authentication mechanism that limits the accessibility to the critical data. This mechanism will ensure that only privileged members who have the encryption and decryption keys can access the stored content. The secured storage scheme shows great results in terms of privacy preservation and data confidentiality.

- **Scheme design features**

Ganapathy, S et al. scheme has a straightforward system structure. Multiple layers shaped the scheme's design, including user interface module, cloud database, data collection module, decision manager, secured data storage model, and key generation model. The user interface module represents the first layer that allows users to communicate (send/receive data) with the cloud database and the rest of the system modules. In addition, every user has his own reserved space inside the cloud database, which gives them the absolute freedom to store data in both encrypted and normal format. Also, the data collection module operates in a way that focuses on gathering user requests that arrived through the user interface module and redirected these requests to the decision manager.

Furthermore, one of the most important modules that play a sensitive role in the overall system is the decision manager because it supervises all the operations performed in

the modules and governs all the modules inside the system. In addition, we must also mention that user data must enter the secured data storage module for the purpose of encryption and decryption so that it can be stored inside the cloud database. Then, whenever a cloud user sends a request to the data collection module, the request will be redirected to the key generation module, which in turn generates the keys for the respective user. Lastly, the user can gain access to the desired data whenever he receives the keys and performs the decryption process.

- **Mathematical approaches**
  - Chinese Reminder theorem

    The Chinese Remainder Theorem (CRT) [46] is a number theory that states if one knows the remainders of the Euclidean division of an integer n by several integers, then one can determine the remainder of the division of n by the product of these integers uniquely, under the condition that the divisors are pairwise coprime. The purpose of using CRT in this scheme is to generate the required algorithms (secured storage algorithm and key generation algorithm) that secure and control the access user's data located in the cloud.

- **Encryption and Decryption process**
  - **A secured data storage module**

    The algorithm started by choosing plaintext as input. Then, it uses the CRT theorem to calculate variables, which in turn will be used as an input for the encryption formula. We must mention that there are two main encryption techniques used in the secured storage algorithm. The first one is the Caesar cipher technique [47] and the second one is the proposed encryption formula:

    $$\alpha = Kg + \mu \quad (1)$$

    In addition, in order to save cloud user data in an encrypted form inside the cloud database, it must first enter the Caesar cipher encryption algorithm; then, the second encryption stage must be performed in order to complete the whole

encryption process. The second encryption process is executed by applying the proposed encryption formula. Therefore, data will be ready to enter the decryption process, which uses the proposed decryption formula:

$$\delta = (\alpha mod\ N) - 1 \quad (2)$$

Finally, the result obtained from the decryption formula will be processed in parallel with the result obtained from the Caesar cipher array to acquire the original text.

- **Key generation algorithm**

In this algorithm, the process of key generation started by choosing the number of users who want to gain access to data located in the cloud database by sending requests to the key generation algorithm. As soon as the requests reach the key generation algorithm, a random public key must be picked (process inside key generation algorithm) so it can be used in the encryption process to encode the user's data. As we mentioned before in the secured storage scheme, the key generation algorithm utilizes the CRT theorem to calculate multiple variables, which in turn will be used in the encryption formula. Also, another key must be picked for the encryption formula, which is the (Private key). When both keys are picked, and the CRT has calculated the variables required to begin the encryption process, the process starts by calculating the proposed formula. Then, after completing the encryption process, the resultant ciphertext will be used as input for the decryption process along with the public key. The outcome of the decryption process will be the private key that needs to be delivered to the cloud user separately to help them access the desired data.

- **Scheme Implementation**

The scheme is developed using Java programming language. The implementation of the scheme has been achieved using the Intel Core I7 CPU system along with 8GB of random-access memory and 500GB of a physical hard disk drive.

Also, the implementation has been adopted in windows server 2008 for making a group of 1000 cloud members. Moreover, CloudSim with Eclipse has been designed to serve as a cloud environment [48].

- **Performance analysis**

The secured storage and key generation algorithm are the main parameters to evaluate the scheme's performance:

- **Secured storage performance analysis**

Apparently, Ganapathy, S. et al.'s scheme shows promising results in terms of encryption/decryption time compared to other schemes that use RSA, AES, and DES cryptographic algorithms [49]. Although this scheme uses a 1028-bits plain text size and a variety of key sizes used in the implementation process (64, 128, 512, and 1028-bits), the results were significantly better when using the CRT-based secured storage scheme over the rest of the schemes. The results of the time taken for the complete encryption/decryption processes were about 0.403425/0.398783 compared to other schemes, which were for RSA= 0.413212/0.401533, AES= 0.55000/0.5402866, and DES= 0.582345/0.574246, all measured in a millisecond.

- **Key generation algorithm performance analysis**

The key generation algorithm has taken into consideration two parameters to measure the performance. First, the computational time to generate encryption/decryption keys. The results show that Ganapathy, S et al. scheme required a small amount of time to perform both encryption and decryption processes compared to other schemes. Even when Ganapathy, S et al. scheme uses different types of key sizes, it still achieves the lowest amount of time to execute the encryption/decryption processes. All the previous results have been obtained since Ganapathy, S et al. scheme choose high-efficiency method (CRT theorem) to select prime numbers and due to the perfect utilization of the Caesar cipher method according to [47]. The second parameter is the security analysis. Ganapathy, S et al. scheme has achieved a high-security level between 98%-99%

compared to other schemes that barely reach 98%. All the previous results have been obtained based on the implementation of perfect cryptographic methods that can deal with different types of key sizes.

2.3.4 T. Subha scheme for privacy preservation and data purity analysis in cloud storage

Over the past years, many researchers tried to design schemes that can address the threats caused by Man-in-the-middle attacks. Fortunately, after a few years of research in the field of cloud computing, a novel scheme came to life to resolve the potential threats that may cause the communication between clients and cloud services providers to be insecure. T. Subha et al. proposed a scheme [50] for privacy preservation based on the data purity analysis approach in cloud storage. The scheme aims to improve a recently proposed model that also preserves data privacy and prevents tampering operations on the user's communication with the cloud service provider. The improved version of the previous scheme [51] implements unique methods that assure no one can alter user data during the transmission phase between parties. The adoption of the Digital Signatures [52] along with Certificates [53] ensures that the request and response messages transmitted came from a trusted party. In addition, digital signatures and certificates can be used by the clients (also can be used by other parties such as the Trusted Third Party and cloud service provider) in every communication with the cloud service provider in order to ensure that the transmitted data will not be exposed to potential attacks from malicious adversaries.

- **Scheme structure and workflow**
  - **Scheme design features**

    There is a need to clarify the stages of creating this scheme and its workflow criteria for the third-party auditor. Also, the scheme presents a detailed analysis behind the use of the Digital signatures and Certificates with the communications established between users and cloud service provider:

1- Setup stage: splitting plain data into several segments and adding a signature for each data block.
2- Key generation stage: public and private keys are generated to use later for encryption and decryption purposes. In addition, a random value must be chosen to use later in the generation of Tags.
3- Signature generation stage: to create labels that can identify data files, a unique element called Tag is generated from the combination of a filename and arbitrary value. According to [54], a secret key-based signature is generated for the data blocks to prevent identity and data theft. Also, the scheme uses an incredible algorithm called Merkle hash tree [55] to store Tags and to guarantee the authenticity of data blocks.

- **Auditing and scheme workflow**

When the trusted third-party auditor receives an auditing query from the client-side asking for verification on certain data, the TTPA started to perform several integrity processes to ensure the safety and validity of the transmitted data. The TTPA started the process by sending a challenge message for several data blocks to the cloud service provider. The challenge message must contain the number of blocks and the set of signatures corresponding to each data block. As soon as the cloud service provider receives the challenge message, a proof message must be sent by the cloud service provider to the TTPA and must contain information that ensures the recipient party's authenticity. The response message must consist of two essential parts, the data proof and the cloud service provider signature. These key segments will help the TTPA recognize the other party (cloud service provider), and it can ensure that the message came from an authenticated contributor in the system. Lastly, after the reception of the response message from the cloud service provider, the TTPA needs to make sure that the contents of the response message are valid and came from an eligible end. The TTPA runs a special algorithm to verify data purity by comparing signatures stored in this system for the same data blocks with the newly created signatures from the cloud

server. Usually, if the verification process was a success, it means that both signatures are identical; otherwise, it rejects the response message.

- **Digital signatures and online certificates implementation**

  Digital signatures and certificates are added to the system in order to secure the data being transmitted, prevent any attempt to tamper or replace the original data, and to check whether the cloud service provider is authentic or not. The implementation of the digital signatures and certificates is executed by a special protocol located in the TTPA. Digital signatures help the certificates link a unique piece of information (including personal information, user id, IP address, and password) to the public key used for the encryption of a specific number of blocks; therefore, gaining access to user data will be almost impossible without the proper identifications.

  The implementation of digital signatures and certificates starts at the client-side. During the execution of key generation, a certificate must be obtained by the user from a certificate authority to send it together with the public key to the TTPA to start the authenticated communication with the cloud service provider. However, the user needs to verify the probity of the certificate before establishing any connection with TTPA. The verification can be achieved using a special algorithm that verifies the digital signature obtained from the certificate authority. In addition, the user needs to pass the verification algorithm using a secure channel to the other parties involved in the working system (TTPA and Cloud service provider). This step is very important for ensuring secrecy between contributors while establishing communications. It eliminates the threat when the attacker behaves as a genuine client to gain access to data. As soon as the verification process of certificates complete in the involved parties, the TTPA starts to establish communication with the server (cloud service provider), creating a secure channel encrypted with a session key shared between both parties.

- **Proof generation**

  The cloud service provider initiates the generation phase of the proof (the response message) using the previously generated secret key to reply to the coming challenge message. Here the proof message must contain the proof (containing recognized information for the other party to ensure server authenticity), the cloud service provider's newly generated signature, and the certificate.

- **Verification process**

  The last step in the scheme workflow is the verification process of the response message (proof message) conducted by TTPA. The first verification process is to check whether the server's certificate is genuine or not, and the second verification is to check whether the signature belongs to the rightful party. The second verification uses the public key generated previously in the key generation phase resides in the client-side for decrypting server signature.

- **Performance analysis**

  T. Subha et al. scheme has been designed and executed using the Eucalyptus tool. Eucalyptus fast start version 3.4.1 [56] on Centos6 has been installed on Intel core i5-3520 CPU at 2.2 GHz, together with 500 GB of a physical disk drive and 8 GB of Ram.

  There are three distinctive parameters used to measure the efficiency, performance, and privacy of the scheme:

  - Auditing time against the number of blocks: the auditing time achieve a sustainable level of performance (above 95%) against the number of blocks being audited.
  - Communication costs against the number of blocks: despite the results founded in the scheme that shows an increase in the communication cost in a linear form, the scheme's communication cost is lower than the one in other systems that use different types of encryption/decryption methods.

- Privacy preservation performance: T. Subha et al. scheme maintains the privacy of users above 95% when active adversaries are involved in the system. T. Subha et al. scheme can detect changes in the stored data.

2.3.5. Yu Jin et al. scheme for privacy preservation and data hiding in cloud storage

Yu Jin et al. introduces an enhanced version of the first Lagrange interpolation scheme to build a better privacy-preserving solution that properly implements the data hiding principle [57]. The new scheme combines the features of data confidentiality and service availability in a single model, which adopts the Lagrange interpolation [58] method that can serve as an encryption/decryption method to preserve the privacy of the stored information in the cloud storage. Also, the Lagrange interpolation scheme uses the principle of data hiding instead of referring to external assets such as Reed-Solomon coding to hide sensitive data. The Lagrange interpolation scheme has a unique feature of using a multi-cloud storage system to store the client's data. The Lagrange interpolation scheme can split the client's data into several blocks and distribute them to multiple storage environments. This operation can ensure no data theft could be occurred by adversaries from the multi-cloud storage system. The improved version of the Lagrange interpolation scheme has proven to be efficient and secure. The scheme maintains multiple security properties such as data confidentiality and better allocation of server resources. However, not every privacy-preserving scheme has the full potential to protect user's data, but at least it can minimize the overall security impact on user's private data.

- **Scheme structure**
  - **Lagrange interpolation definition**

    For a given set k of data points (x_0, y_0),…., (x_1, y_1),…..,(x_k, y_k), an interpolation polynomial L(x) can be built by using these data points. other n variables (n>=k) independent variables a_1, a_2, a_3, a_4 are substituted into the

polynomial L(x). So, the y_1,y_2,y_3 will be inserted into the $L(a_1)$, $L(a_2)$, $L(a_n)$. If arbitrary k data point $(a_k,L(a_k))$ together with x_0,x_1,x_k are obtained, the original $y_0,y_1,\ldots,y_k$ can be recovered [58].

- **Scheme design features**

The design of the Lagrange interpolation scheme is based on using the multi-cloud storage system. So, the improved version of the system will consist of two main operations:

1. **Store data into the multi-cloud system**

The client-side starts the data upload process by splitting the original data block into multiple data segments to fulfill the requirement of the Lagrange interpolation algorithm. We must mention that there is a small requirement to fit the data block into the multi-cloud system. The data blocks need to be a multiple of three, so it can be compatible with the multi-cloud storage. If the original data is not a multiple of three, it will be forced into a container that has a size of 3 bytes. Follows that, the user needs to perform the Lagrange interpolation algorithm on the original data to generate four data blocks (the fourth data block to create the redundancy that ensures the service availability). As we mentioned earlier, the data points (x_0, y_0), (x_1, y_1), $(x_2. y_2)$ will help to generate the interpolation polynomial. Later, the user needs to insert four random variables and merge them into the polynomial to hide the original data segments within it. Finally, the user can upload the data segments (the result obtained from the data hiding process) to the multi-cloud servers.

2. **Retrieve data from the multi-cloud system**

The client sends a retrieve request to the multi-cloud system. Then the server responds to the client by sending the access permission of the desired data. As soon as the client receives the response from the server, the client starts to download the data segments generated as an effect on the

store process. Later, he receives the original variables used with the original data blocks to construct the polynomial that can refer to the (decryption key) from the file owner so he can decode the hidden data and gain access to the desired files. Finally, the user must perform the Lagrange interpolation algorithm to restore the data segments into their original form.

- **Implementation and performance analysis**
  - **Implementation**

    The implementation of the Lagrange interpolation scheme has been conducted using the Java programming language. The scheme uses four Cassandra [59] cloud databases and adopted an SWT [60] for the design of the system interface.
  - **Performance analysis**

    The scheme adopts three parameters to measure the performance and efficiency of the system:

    1. Data confidentiality: at first, the adversary could seize the first part of the information from the multi cloud-system. Although he gains access to the first part of owner data, he cannot reveal the rest of the data. Therefore, in this situation, security or data confidentiality has been approved. Secondly, the adversary may attack the multi-cloud system and target only two clouds to gain access to two parts of the data. According to the Lagrange interpolation equations [61], it has been proven that this part is also immune to security breaches adopted by attacking two cloud servers in the multi-cloud system. Lastly, the adversary may attack three cloud service providers (three clouds located in the multi-cloud system) and gain access to the three data points. Although these data points can construct the polynomial, the security trick here uses the original variables (decryption key) to conceal the original data from the manipulation attempts. Unfortunately, this situation has a backdoor gap.

The problem occurs when the adversary tries many decryption keys to decode data points and recover the original variables used to construct the first interpolation polynomial.

2. Time Consumption in upload and download operations: Yu Jin et al. scheme has been compared with another algorithm called DEPSKY-CA [61] that uses the AES symmetric encryption technique. The results show that each algorithm conducted five types of data size (10KB, 100KB, 500KB, 1MB, and 10MB) to conduct this operation. For the data upload, the results proved that the Lagrange interpolation scheme needs the least amount of time compared to the DEPSKY-CA. For the download operation, the Yu Jin et al. scheme requires less time than the other scheme.
3. Storage space: MCDB has a special algorithm to handle data to cloud storage [62]. So, the data will be filling each cloud storage. While the old Lagrange interpolation scheme and the improved version store one-third of data in each cloud. The results show that the MCDB mentioned in [63] needs much space compared to the old Lagrange interpolation scheme and the improved one, which needs less space.

2.3.6. Zhen Yang et al. hash-based scheme for confidentiality and accountability in cloud storage

Zhen Yang et al. introduce a hash-based privacy-preserving scheme [64] as one of the unique schemes that focus on achieving the concept of confidentiality for the data outsourced to the cloud service providers. Zhen Yang et al. adopt a unique authentication model that implements the hashed client aliases feature to protect the user's private data. The authentication tool has been re-developed in a way that allows it to implement the hashed client aliases and data identifier, which achieve privacy-preservation property. Therefore, the data content will be kept secret from any manipulation attempts done over the auditing process. Also, confidentiality-based

certificates [65] have been introduced to help overcome the attacks that target data confidentiality. In the earlier schemes, data auditing has been presented to discover unauthorized access attempts to the cloud networks by malicious adversaries. Unfortunately, the auditing process requires a specific number of resources and a huge effort from users to implement. Therefore, Zhen Yang et al. uses an auditing tool that oversees the communications established between data owners, clients, and cloud service providers and secures it in a way that prohibits any outside attempt that threatens data content. The public third-party auditor [66] has been introduced in this scheme to overcome the threats of modification and manipulation of the user's data stored in cloud data storage. The adoption of the third-party auditor gives the user the ability to handover the auditing task to a special party involved in the working system that assures the secrecy and concealment of the owner's sensitive information and at the same time eliminates workload from normal users.

- **Scheme design structure**
  - **The structure of the Inspection model**

    There are four main algorithms that shape the structure of the Inspection model:

    1. Hash Identity to create client aliases for every person registered in the system. And this is done by the data owner.
    2. Authentication tool to create unique certificates, and it is adopted by the cloud service provider.
    3. Access Identifier based on the received certificate is generated by the cloud service provider. The access identifier builds the clients' access list, and this operation is executed by the third-party auditor.
    4. Data Loss checker checks whether the incoming and outgoing communications result in data loss.

- **Inspection model workflow**

At the beginning of the inspection process, each client is given a private and public key to access the user's data, so we can assure that the encryption infrastructure of the scheme is based on the public-key encryption approach [67]:

  - Initialization phase: a broadcast encryption technique [68] is used by the data holder to encode data and manage the key distribution. Also, for every client contributing to the network system, a hash identity is allocated for each client so that they can be recognized by the data holder for future processes.
  - Data inspection: a read request along with the hashed identifier for the authenticated client is sent to the CSP. This request informs the server that a client is asking for permission to access the owner's data. Then CSP generates a certificate after checking whether the person who asks for the data access is an eligible user or not. The user receives the certificate from the CSP and starts the validity test.
  - Trusted third-party inspection: the data holder needs to investigate whether the certificates are valid or not. So, he delegates the trusted third-party to recover the certificates from the cloud service provider. Then the certificates are compared with the access list generated by the Access Identifier to find the privileged clients. In the end, an inspection report will be formulated based on the results from the trusted third party and a Data leakage check.

- **Main schemes and design properties**
  - **Client identity concealing**

Zhen Yang et al. scheme adopts a hashed identifier to conceal the identity of the clients involved in the cloud network. This scheme uses a special technique to hide the original identity of the clients contributing to the communications and revealing only the hashed identifier for the rest of the network parties. The technique involves creating a list of client's identifiers known only by the data holder. Therefore, the hashed identifiers

will be distributed to other entities using the broadcast encryption technique. Zhen Yang et al. says that to generate the hashed identifiers, *"With random permutation, UserID is converted to RandomID. The SHA-1 hash of RandomID is the HashID"* [64]. Clients will be registered in a list kept by the data holder, which contains client identifiers (including client id, arbitrary id, and the hashed id) and a version number that refers to the list version with a numerical value. Furthermore, the hashed identifier list will be sent over an encrypted line to the CSP along with its version number to inform the server of the list of the trusted clients who are already registered in the system. At the same time, each client will be receiving his identifier along with the decryption key so they can be able to read data from cloud data storage.

The client identity concealing technique has a few properties:

First, the data holder needs to issue a re-encryption process with a new key whenever a new member got added to the clients' list. This process must be followed by the client identity concealing process to hide clients' identification information from other parties. Secondly, the data holder is complied with altering the hashed identifier periodically to confuse the other party and prevent any attempt to reveal the original identity of the client. Lastly, the cloud service provider can send data to the clients only if the cloud service provider can verify successfully that the version of the hashed identifier's list has been updated recently.

- **Confidentiality-based certificates**

  The idea behind taking the certificates [65] as a basic technique to shape the hashed scheme is that it offers the data privacy and the confidentiality needed to establish a secure line between clients and cloud service providers. The structure of the certificates contains:

  1. Hash block identifier: every data block has its unique identifier that can be shared between clients.

2. LSN: is counter attached to the hash block identifier that increments by one whenever there is an attempt to reach a specific data block.
3. Block hash: contains the hash value of a specific data block.
4. User hash identifier and version number: personal identification information for specific clients registered in the system.
5. Timestamp: the current access time of the certificate.
6. Chain hash: this field contains the chain hash value of the previous certificate and the one currently being processed. We must note that if we want to ensure that only the third-party auditor and clients can check the certificates' integrity, the cloud service provider must encrypt the generated certificates with his private key to ensure the confidentiality feature.

- **Probity Inspecting**

Zhen Yang et al. explain an equation that ensures no attempt to tamper certificates shall occur *"if verify(pk_{csp}), $signature_i = hash_{sig}$ (data || chain hash) passes, the ith attestation is intact."* The probity inspection tool offers a solution to check if there are any incorrect values in the fields of LSN and chain hash that result in certificate loss.

- **Bifurcation examination**

Usually, cloud service providers try many ways to interrupt communications between cloud parties to gain access to sensitive information. So, when it comes to certificates, the cloud service providers attempt to hide one of the successive certificates during its transition to the clients to make a gap that can be used later for fraudulent and tampering acts. However, the positive thing in this scheme is the use of the LSN (local sequence number) that can be utilized as a marker to prevent any manipulation attempts by the CSP.

- **Access table**

  Upon returning the certificates to the third-party auditor, the certificates must be translated into a simpler form to create the access list. However, the access table generation relies on an important factor, which is the integrity and validity of the certificate itself.

- **Trusted third-party workflow**

The process begins on the client-side (data holder). The data holder starts the process by initiating an inspection request and send it together with the authority table and the hash id table to the third-party auditor. Then, the trusted party asks the cloud service provider for the certificates to establish the probity inspection. The trusted third-party auditor inspects the incoming certificates for any untrusted or unlicensed access and reports that to the data holder.

- **Rapid inspection process**

  The TPA uses two tables to supervise clients‘ access to the system: The authority table and the access table are used as parameters to check the validity of the clients ‘list. However, the authority table must be generated at the beginning of the inspection process, while the access table must be generated by the trusted third party due to the use of the confidentiality-based certificates technique. Lastly, an inspection report is generated by a trusted third-party to allow the data holder to verify the safety of his private data.

- **Implementation and analysis**
  - **Experimental tools**

    The implementation of the experiment has been adopted using different specs. The data holder used an Intel Celeron N3050 CPU along with 2GB of Ram, while the trusted third-party auditor used higher-end hardware, including an Intel Core I5 5257U CPU along with 8GB of Ram. The cloud service provider used a multi-cloud server system to conduct this experiment.

Also, we must mention that the network environment used to apply this experiment is the Local area network, where the perfect connection setup is ensured between the entities.

- **Performance analysis**

The hash-based scheme has taken into consideration three parameters to measure and evaluate the privacy and performance aspects:

- **Time cost for initialization and setup**

The results show that the number of clients is an influential factor for the time cost in the initialization and setup phase of clients' aliases. The results show that for 10000 clients, the time needed to set up the client aliases for each person is around 0.4 seconds. Therefore, this will affect the privacy factor, which will escalate significantly due to the minimum use of computation during this process.

- **Inspection performance**

The assessment of the hash-based scheme was built based on four key techniques conducted in the essential scheme:

1. Performance of probity inspector: the focus of this assessment is to evaluate the chain hash field that plays a unique role in probity and bifurcation checking. The total number of certificates will have a noticeable impact on the chain hash inspection. The results show that the cost of performing an inspection process over the chain hash field will cost around 15.84μs. Although Zhen Yang et al. has adopted parallel processing to decrease the computation time of chain hash inspection, it appears that the increasing amount of threads handling will make parallel processing a tough and inefficient task.
2. Performance of bifurcation checker: Zhen Yang et al. have explained the efficiency of bifurcation checker, *"we suspect that in a series of attestations whose length is p, the kth attestation's chain hash error has*

resulted from forking, where k is uniformly distributed from 0 to p/1 with a probability of 1/p. Then the forking checking complexity is O(p)".

3. Performance of unlicensed access detection tool: the unlicensed access detection tool uses two features to measure its efficiency. First, the results show that with the expansion of the user group, the time cost to detect unauthorized access to the cloud data significantly increases. Also, the detection speed of unauthorized access has been decreased due to the clients' growth.
4. The second factor is the number of certificates used during the auditing process. Zhen Yang assumes that the number of certificates used during the auditing process between 10^5-10^7. They also suppose that the number of clients registered as an authorized client around 10^4. The results show that the relation between the detection tool and certificates is based on direct proportionality, and the cost for a single certificate inspection around 24.8µs.
5. Performance of client liability: the hash id and version number of the hash id list determine if there is any loss in user data during the auditing process with the help of client id. The results show an increase in search time when the trusted third-party tries to detect unusual or suspicious access to cloud data compared to the search time of the data holder. In addition, the results show that for a clients' list with a size of 10^4, the search time will be almost ten milliseconds for each party to ensure client liability. In terms of the client liability cost, with the use of a different number of certificates, the difference between the trusted third party and data holder is barely noticeable. The generation of the access table in the rapid inspection phase results in a list that holds a piece of unique information that ensures client liability.

- **Inspection cost**

The inspection cost evaluation is adopted over two systems: a system with data holder and the cloud service provider only and another system with a third-party scheme which involves data holder, TPA, and CSP. The results show that in both situations where a data loss occurred or not, the inspection cost stays balanced with no significant change. However, the effort to conduct the inspection process for data holder has shown no impact on the third-party scheme's efficiency in the situation where there is no data loss occurred during the inspection process. Also, the results show that the data holder requires lesser effort to conduct the inspection process where there is a generation of false certificates due to incorrect or unusual access to cloud data. In addition, the unique abilities of the third-party scheme reduce the effort needed from the data holder to perform the inspection process. Therefore, the third-party auditor performs most of the job, which creates a downside on time cost. The results show that if the scheme uses 10^6 certificates together with 10^4 number of clients, the time cost ratio between using the third-party scheme and the two-party scheme will be around 20%. Also, the increase in the certificate number will significantly affect the third-party scheme's time cost.

The results show that if the number of certificates increases from 10^5-$10^{7,}$ the time cost ratio between using the third-party scheme and the two-party scheme will decrease from 85%-8.5%. Furthermore, the communication cost plays a sensitive role that affects the efficiency of the scheme. The results show that for the two-party data holder, the communication cost = O(p) while P refers to the number of certificates. However, the communication cost for the third-party data holder = $O(N_x)$ while X refers to the version number of clients' list. Finally, the communication cost for the TPA in a third-party scheme = O(p).

2.3.7. Liu Guoxiu et al. secure database scheme with triple encryption system for privacy preservation in the cloud environment

Liu Guoxiu et al. [69] proposed a privacy-preserving scheme based on the secure database approach for protecting data privacy and cloud storage contents. The scheme presents a unique and practical privacy-preserving solution to create a confidential and private cloud database environment. The idea behind designing such a scheme is to build a secure cloud database that can apply and execute SQL commands over different types of encrypted data. Liu Guoxiu et al. proposed a triple encryption system to increase the security level and enhance the overall performance characteristics of the entire scheme when encrypting plain data. Also, The uniqueness in the design comes in the fact that SQL commands can be executed over any type of encrypted data without an extra burden on the user or cloud service provider and to focus the workload on the cloud server only. The experimental results show significant improvements in the computation overheads for encryption and decryption processes while at the same time, attain the privacy-preserving property of the outsourced data.

- **Scheme structure and encryption models**
  - **Cryptographic techniques**

    The main purpose of using encryption techniques is to provide a secure environment where data owners and clients can interact with database content without exposing the privacy of data to security risks. However, the use of common database encryption techniques creates difficulties in providing a privacy-preserving database because of the amount of randomization in the resultant data that ruins the initial order. Also, many SQL operations will not be executable due to the use of regular encryption techniques. Furthermore, G. Liu et al. considers possible attack models that can jeopardize the privacy of data. In the first model, attackers may gain access to the cloud database and expose data content. This model is referred to as the Ciphertext-only attack [70]. In the second model, which is referred

to as a Chosen-plaintext attack [71], the attacker may have the knowledge to predict private and public keys used to encrypt the data. However, the attacker must have previous knowledge about some security properties of the data before conducting this type of attack. The secured database scheme utilizes three different models to build a system with a high level of security expectations:

1. Two-layer encryption model: the formation of this model is based on two types of encryption techniques. The first one is arbitrary encryption; this technique is shaped using the block cipher encryption technique with an arbitrary variable called salt. The combination of several keys, including master key, column identifier, and row identifier, results in the salt variable. Also, the client-side is responsible for generating the salt variable. Secondly, the deterministic encryption technique is formed from combining the block cipher technique with the ECB mode [72]. In deterministic encryption, clients use the key generated by taking the pseudorandom permutation function of the master key and the column name to encrypt values in a specific column.

   The implementation of the techniques is performed in two steps; the first step is the encapsulation of table values with the deterministic encryption, then the client encrypts this form with the arbitrary encryption. However, if clients want to perform the select command with equality predicates, he needs to decrypt the exterior layer by transmitting the decryption key for the exterior layer to the cloud server before conducting select command; otherwise, table values will keep the original encryption form.
2. Monotonic encryption model: monotonic encryption model used to encrypt the floating-point numbers using a unique scheme that deals with the float number. Liu. D described the non-linear monotonic scheme in his paper. By taking the sensitivity of value v, the monotonic encryption scheme is a function f:

$$nindex^{sens}_{[a,b,f]}(v) = a * f(v) * v + b + noise \quad (3)$$

*"where x is a plain text, a and b are secret, and noise is a randomly selected value. The order-preserving property means that for all v1 and v2, if v1>v2, then a*v1+b+noise1 > a*v2+b+noise2"* [73]. monotonic encryption model assures to keep the original sequence of the plaintext untouched, and at the same time, it can be executed over the range queries of SQL.

3. Homomorphic encryption model: it supports the encryption of the float numbers like the monotonic encryption model [74]. While addition and multiplication commands of SQL database are supported in this model. The homomorphic encryption model has used a previously designed encryption scheme proposed by D. Liu. The following representation will describe the scheme: let v be the float number meant to be ciphered, n represents the number of the sub-cipher text, and K(n) will represent the key. The encryption of v using the key K(n) will result in the ciphertext. However, each sub-ciphertext must fulfill the equation:

$$C_i = value_i(k(n), v) + noise_i(k(n), R \quad (4)$$

Based on the original equation [75], *" each sub-ciphertext may comprise adding a first result and a second result, where the first result is the value of a function based on a key associated with that sub-ciphertext and the numerical value, and the second result is the value of a function based on the key associated with that sub-ciphertext and one or more random numbers."* However, A linear time complexity may occur between functions based on the number of sub-ciphertexts. The decryption equation comprises the key and the ciphertext that consist of several sub-ciphertexts.

- **Performance evaluation**
  - **Implementation tools**

    The implementation of the secured storage scheme has been performed using Cent OS with the Java programming language. The system used to evaluate the performance and efficiency of the scheme consists of an Intel Xeon CPU E3-1226 processor with 3.3GHz and 16 GB of RAM.

  - **Security achievements**

    Two types of attacks, ciphertext-only attack, and a chosen plaintext-attack are used to evaluate the security achievement of the scheme:

    1. Ciphertext-only attack: the use of the triple encryption system results in a secure database that is impenetrable by the ciphertext-only attack. The randomization and probability in the first encryption model prevent any attempt to attack the database storage using the ciphertext-only attack because identical plaintext values are assigned to dissimilar ciphertext. The use of the monotonic encryption model adds a level of complexity to the ciphertext due to the use of the data indexes concept. Also, the use of the nonlinear order-preserving scheme made it impossible to expose the secured database scheme to the ciphertext-only attack. Furthermore, the homomorphic encryption model has an effective role in securing the database. The functionality of the homomorphic encryption model is to yield various results even if the encryption occurred for the same data and with a single key. The noise added to the ciphertext in the second equation introduces more tangled data that makes it more difficult for the attacker to retrieve the original data.
    2. Chosen-plaintext attack: in this type of attack, the adversary may collect a random number of plaintexts to analyze and decipher. However, if the adversary finds out some of the plaintext segments and tries to launch the chosen-plaintext attack, he might get the information about the

decryption technique used. However, he cannot find out the private key used to encrypt the original data because each pair of data encrypted with the triple encryption system will results in dissimilarity in the ciphertext even if the key used to encrypt the pair is identical.

- **The execution time of encryption models**

  The evaluation of the triple encryption models is conducted based on the average execution time of each model. The results show that the Two-layer encryption model has achieved a 12 us compared to other encryption models used in the same system and result in a lower average of the execution time. However, both the monotonic encryption model and the homomorphic encryption model have a minor difference in the execution time due to the level of complexity, which is almost *O(n)*.

- **The execution time between SQL operations and the proposed scheme**

  A comparison of SQL operations versus SDB operations has been adopted to assess the performance level between two database environments. The test has been performed using basic SQL queries. For the insert and delete queries, the average execution time of these operations in the SDB environment yields almost the same results without the encryption process. In terms of the select query, the execution time of the encryption is close to the execution time of the decryption operation due to the elevation in the number of queries. Finally, the update query has shown an increase in the amount of time needed to execute the query over encrypted data.

- **Performance analysis between SDB and CryptDB**

  A comparative analysis has been conducted between the SDB and CryptDB (an earlier proposed database scheme for privacy preservation) [76] to evaluate the secured database scheme. The comparison has considered two parameters to evaluate the performance between schemes:

- Processing cost: the results show lower processing time when using the SDB scheme compared to the CryptDB because SDB uses the triple encryption system that allows for a robust and efficient way to encrypt data in a smaller amount of time with a lower processing cost. While CryptDB shows opposite results to SDB because CryptDB uses a multiple layer system that increases the execution time and increases the processing cost, which adds a time delay to the system.
- Storage space: the results show that the SDB scheme has a significantly lower usage in storage space in comparison with CryptDB. Although both schemes have shown a negative effect on the storage space of DBMS in terms of amplifying the amount of the encrypted data stored, SDB proves to be more efficient and uses a small storage space.

CHAPTER 3

PRIVACY ATTRIBUTES AND THEIR SIGNIFICANCE

3.1 Introduction

The remarkable growth in the sectors of electronic and digital globalization has had an effective influence on integrating security and privacy concepts in various areas of life. Experts in the fields of internet and cyber-security determined to extend the sphere of knowledge on the concept of privacy given the crucial importance it possesses. The study focuses on understanding the nature of privacy infrastructure and harvesting key-features and attributes. These attributes can be utilized to minimize the severity of privacy violations. Relativeness is considered an important characteristic of privacy that means every entity has its unique relationship with privacy, while Affiliation means that the privacy of an entity belongs to that entity only [77]. However, with the rising technology of cloud computing and its ability to deliver a comprehensive bundle of services, privacy-preserving techniques experts started to realize the importance of privacy attributes and its capabilities to augment a secure infrastructure to their models and schemes.

In the beginning, there was a limited amount of information and resources about the correct methodology for obtaining such features and attributes. So, basic attributes with limited functionalities started to emerge due to the use of classical extraction techniques. However, confidentiality and universality are considered to be the traditional attributes for privacy, where confidentiality refers to the act of keeping sensitive information as safe as possible. In contrast, universality refers to the people's perspective about privacy and how an individual sees information and claims it to be

his own among other people [78]. Furthermore, the fast-passed evolution in the cyber-world and the huge demand for cloud computing services create a big leap in the cyber-security industries. Privacy attributes refined and evolved in various ways, including type, nature, and security achievements. Modern features and attributes such as integrity, accountability, availability, and preservability are introduced as the new pillars for privacy [79]. These attributes made the inspection and evaluation of privacy-preserving techniques an effortless task by incorporating robust and effective capabilities.

This chapter focus on gathering the most advanced and iconic privacy attributes used in privacy-preserving techniques that address cloud storage violations. These attributes are considered to be the latest findings of the field experts in the cyber-security domain. The attributes of privacy-preserving techniques include Data Auditing approaches, Cryptographic techniques, External algorithms, Key generation mechanism, Key management, Key length, Key function, Design features, Performance standards, Type of attacks, Attacks addressed, Test environment, Tests applied, Cloud-storage structure, Abnormality, and Security achievements. The emerging technology of cloud computing requires integrating accurate techniques to raise security levels within cloud storage. These attributes can support the structure of the privacy-preserving techniques by providing the necessary features, which grant the security layers to protect the user's privacy in cloud storage. However, the research performed over these attributes will help future researchers to evaluate and improve existing techniques. Also, this research will allow cyber-security experts to extend the search for brand-new privacy attributes, which can strengthen the foundation of privacy techniques in the coming future.

3.2 Utilization and significance of privacy attributes

Privacy attributes have become very important after the implementation of cloud computing worldwide. These attributes have become the foundation stone for the concept of privacy-preserving for sensitive data in cloud computing [80]. Data

auditing approaches are used to assess and observe cloud security policies and mechanisms to ensure that it functions securely and properly [81]. In terms of cryptographic techniques, encryption and decryption mechanisms provide protection for the user's private data against security attacks without compromising the efficiency of the data connection line [82]. External assets are uniquely important in a privacy-preserving scheme's design. It allows designers to integrate more functionalities and properties to enhance the scheme's security and performance. Key generation mechanisms and key-length provide the cryptographic techniques with compound key generation utilities and complex keys to add a degree of complexity to the encrypted data [83]. In the same context, Bruce Schneier described key management as *"key management is the hardest part of cryptography and often the Achilles 'heel of an otherwise secure system"* [84]. The key function is another important attribute that deals with the type of cryptographic key activities such as encryption, authentication, verification, and digital signature. It is one of the important attributes that determine the security level of the privacy-preserving system. For the design features, one of the important aspects of achieving a secure system with privacy-preserving ability and data protection is the adoption of design strategies [85]. Furthermore, performance standards or (performance measurements) can uncover the pros and cons of designing privacy-preserving techniques, allowing developers to improve the design's structure through several iterations [86]. In terms of security and preventative measures, the threat type is also added as an evaluation attribute for the type of security and privacy attacks, which can determine the nature and severity level of the perils. Threats addressed attribute security, and privacy experts must build a long-term security system that can withstand and recover from security breaches. The security system must be able to address a variety of security violations by introducing essential and impactful features, including upgradability, reliability, preventability, and recoverability [87].

The test environment is a very important element in measuring the performance and efficiency of privacy-preserving techniques. The test environment contains two major

elements: the test hardware and test software. Test hardware parts must be gathered from a trustworthy manufacturer, guaranteeing that test equipment is built from high-quality components, which will perform the intended task properly [88]. In the same context, the test software is an essential tool to evaluate system functionality and productivity, where efficiency, flexibility, and preservability must be the core approaches for the test environment [89]. Test software plays a significant role in the design of privacy-preserving techniques. It offers a rich environment that supports multi-function feature, which gives the capabilities to develop an efficient and flexible system. That is why privacy-preserving techniques experts choose unique programming languages such as Python, Java, and C# to write code privacy-preserving techniques. The test applied attribute gives researchers an insight into the scheme's performance in terms of security, computation time, computation cost, and efficiency. The test applied attribute creates a clear image for security researchers about a specific system and gives them the results needed to improve or design proper future versions.

In terms of storage, the cloud-storage structure defines the cloud data storage infrastructure. The designers of privacy-preserving techniques can use two types of storage structures, either single cloud storage or multi-cloud storage structure. This attribute gives researchers the ability to determine the cost-effective and efficient type of storage to lower individuals' or organizations' workload [90]. The abnormalities attribute helps distinguish the features and properties of privacy-preserving techniques by referring to peculiar design characteristics. Abnormalities ease the work for researchers and security experts to classify and differentiate between a diverse number of privacy-preserving techniques that may contain several design properties. Security achievements attribute is another type of evaluation attribute. Security achievements are restricted to show the security level of a specific system, and the number of security attacks addressed. In the following subsequent sections, we will briefly elaborate on the common privacy attributes for privacy-preserving techniques:

3.2.1. Data auditing approaches

The auditing process is the method of overseeing and examining several entities residing in a specific environment to fulfill essential standards and regulations. In terms of cloud computing, data auditing is defined as a method for inspecting CSP services along with the incoming and outgoing connections between cloud parties [91]. Where inspection process aims to verify the integrity of transmitted data by using various inspection techniques, including analysis, review, observation, procedures, and so on [92]. Also, data auditing ensures the obligation to the network security standards and policy, which prevents any unusual violations. There are two types of data auditing internal and external (third-party auditor) auditing. Internal audit performs evaluations and assessments on information and services provided by CSP [93]. Internal auditing is performed by the client-side who seeks to measure the security capabilities of CSP, and it offers reliable and secure results. While external audit (third-party auditor) behaves as a dependent entity, which performs evaluations and integrity checks on data exchanged between cloud network parties [94].

3.2.2 Cryptographic techniques

Cryptographic techniques are described as the methods, approaches, and tools used to encrypt/decrypt different types of digital data with the aim of protecting data contents. Cryptographic techniques consist of both encryption and decryption processes. Where encryption is defined as the method of transforming a plain text to cryptic form, which is more secure and reliable to exchange between parties. This process aims to convert the source text into a secret code that can protect any critical information described in the original representation [95]. In terms of cloud security, various encryption algorithms protect cloud data, such as DES, AES, RSA, and Homomorphic encryption [96]. Encryption techniques help make sensitive data confidential, assuring the applicability of secure multi-tenancy, preventive measures against security violations, provide back-up safety assurance for data stored in the cloud [97]. While decryption is the reverse process for encryption. The decryption

process transforms the encrypted data back to the original representation (plain text), which can be recognized easily by humans and machines [98]. In terms of cloud computing, Decryption techniques are used to retrieve encrypted files from the cloud repository (cloud storage) through inquiries from specific clients. Clients need to have the proper privileges and the decryption key to gain access to the intended data.

3.2.3 External assets

We can refer to the external assets as the third-party tools added inside the security system to provide certain functionality to the overall scheme structure. External assets such as algorithms, data structures, mathematical representations, formulas, and other forms of materials can create a huge difference in the performance and security results of the entire system. External assets add a certain complexity level and abnormal features to provide a privacy-preserving scheme with extraordinary security and privacy characteristics [99].

3.2.4. Key-generation techniques

The key generation mechanism is an essential component when it comes to encryption and decryption. The key generation process generates encryption/decryption keys to apply to that data that intended to be ciphered/deciphered [100]. In terms of cloud security, it uses various key generation mechanisms, including symmetric key generation, public/private key generation, and dynamic key generation, to secure the cloud environment from data theft attempts. The key generation mechanism provides the security system with the compound keys to increase its security characteristics. Privacy-preserving techniques with strong key potentials can overcome any attacks that target cloud sensitive data. Even if the adversary has full knowledge of the security system, he will have difficulty discovering the accurate decryption key [101].

3.2.5. Key-length

A cryptographic key is defined as a group of numbers (0 and 1) generated from a key generation mechanism, which can be used by cryptographic techniques to protect

sensitive information [102]. Key length plays a vital role in cryptographic systems and is considered one of the security system's core pillars. There is a massive range of key lengths based on the used algorithms. For example, Symmetric encryption such as AES and 3DES have a range of 128-256-bit key length, while Asymmetric encryption, including RSA, can have a range of keys from 1024-4096-bit key length [103]. However, the bigger the key length, the harder and longer it gets to decipher the encrypted data.

3.2.6. Key management

Key management can be defined as the administration process over cryptographic keys in the security system. Key management can perform diverse activities, including a key forge, key exchange, key use, key replacement, and key disassembly [104]. Key management can be offered in the cloud as a service to keep the process of keys inside the cloud service provider. But data owners cannot guarantee the safety of their keys in the CSP environment. That is why hardware security modules came up to support key management systems and add a suitable security level to the encryption keys [105]. The technology of hardware security modules gave a significant advantage in terms of safeguarding and managing cryptographic keys [106].

3.2.7. Key function

We can define key functions as the activities or the roles in which the cryptographic key takes to provide security capabilities to a specific entity. The cryptographic key may vary in the type and security characteristics it possesses [107]. The cryptographic key has several roles and functionalities, such as encryption, authentication, verification, digital signature, and master key [103]. These functionalities may add unique layers to the security of firewalls to prevent threats such as masquerade, message modification, and other forms of cyber threats.

3.2.8. Design features

We can describe design features as the important elements emphasized by the designer to integrate more details and functions into the working system [108]. Due to the huge demand for delivering secure and multi-function security systems, security experts plan to adopt new security strategies, approaches, and design layers to create a more capable and secure structure [109]. In terms of cloud security, Design features allow field professionals to fuse a diverse number of security characteristics into their privacy-preserving techniques. The proper implementation of security and design characteristics will result in a secure system that can stand against any unusual violations which might endanger the cloud environment.

3.2.9. Performance standards

Performance standards are the factors by which system capabilities and efficiency can be measured. One of the definitions described performance standards as "*Performance criteria are measurable quantities to be used to evaluate the adequacy of trial designs*" [110]. It is important to mention that performance criteria play a significant role when it comes to evaluating system performance and efficiency [111]. Performance criteria help in determining which parts of the system must be assessed to test the effectiveness and productivity of the system.

3.2.10 Threats type

An adversary may try different means to weaken the structure of the crypto or security system to gain access to important data [112]. Understanding the forms of security menaces that will strike the system is an important aspect of creating a risk assessment report. A risk assessment or risk evaluation help the designers of security or privacy scheme to determine the type of attack that might hit the system. Early evaluation of such perils can improve the security and privacy characteristics of the security scheme.

3.2.11. Threats addressed

Threats addressed attribute can be referred to the number of security violations that have been addressed by privacy-preserving techniques to achieve optimal security level. The advancement in cloud computing made the focus on addressing security system vulnerabilities and defects a painstaking task and without any guarantees [113]. Addressing security and privacy threats is an important aspect of security system design. The early discovery of security attacks will help security system designers evaluate the system's structure; besides, it allows them to fix all the defects and close the gaps that endanger system functionality. However, security systems and privacy-preserving techniques will be vulnerable against many types of threats unless designers invest in new technologies that minimize the security menace's overall impact [114].

3.2.12. Test environment

The test environment can be defined as the pieces of equipment (hardware, software, and network) used to adopt the execution and performance measurements of the privacy-preserving techniques. It offers a proper work setup for the designers of privacy-preserving techniques to perform and evaluate testing activities [115]. The test hardware can be referred to as the pieces of hardware used to adopt the implementation and configuration of privacy-preserving techniques. However, uncertified hardware types have a high probability of endangering security systems through the implementation process due to the weak design aspects [116]. Recently, security and design blemishes have been discovered in the leading chip manufacturers, including AMD, ARM, Intel, and Qualcomm, which is unfortunate and costly for these companies [117]. The test hardware is a unique tool to test the efficiency of privacy-preserving techniques. By forcing the designers to consider investing in suitable, secure, and reliable hardware pieces to achieve the optimal security characteristics. The versatility in using a random type of hardware is very dangerous because the consequences of using the wrong devices to test a dangerous environment could be severe, costly, and time-consuming. The test software refers to the medium in which

privacy-preserving schemes are being conducted and tested. The test software is more the same as test hardware because both share the same objectives of ensuring the secure and accurate implementation of the privacy-preserving techniques.

3.2.13. Tests applied

Tests are the most vital activities in the security or privacy system. Usually, after the implementation of a privacy-preserving scheme or any security systems, several performance and security evaluation tests must be conducted. These types of tests assist with revealing security and performance vulnerabilities, possible errors and malfunctions, and potential security attacks that might collapse the scheme functionalities during certain processes [118].

3.2.14. Cloud-storage structure

Cloud storage is considered one of cloud service provider's unique services for storing data. Also, cloud storage has different structure variations, including private cloud, public cloud, and hybrid cloud. But when the subject comes to the preservation of data privacy, there is a more important feature that needs to be covered, which is the cloud storage structure. Cloud storage structure is referred to as the space allocated for the deployment of privacy-preserving techniques. There are two main storage structures for cloud computing, the single cloud structure and the multi-cloud structure, each of which has its own advantages and disadvantages. In the beginning, individuals and organizations used the single cloud infrastructure as an initial multi-service environment and because, at that time, it was more than enough to hold their data and offer substantial services to serve the current needs [119]. However, with the continuous growth in the cyber world and the advancement of the cloud computing field. It was mandatory to embrace the idea of multi-cloud infrastructure. Multi-cloud infrastructure can be described as "the use of multiple cloud computing and storage services in a single heterogeneous architecture" [120]. It also means that cloud resources are shared among multiple cloud-servers. Multi-cloud infrastructure offers modern and advanced possibilities in terms of security, accountability, availability, and reliability. The

importance of using a multi-cloud infrastructure is that if an organization wants to use a service from a different type of service provider, multi-cloud infrastructure removes any constraints in the face of using a distinctive number of services from different service providers because of its flexibility [121].

3.2.15. Abnormality

Normally, we describe abnormality as faulty or harmful behavior that affects any normal entity. Also, abnormal behavior can be described as the behavior in which it is unusual and deviated from the traditional form [122]. In the context of privacy and security models, Abnormality can also refer to the design characteristics, properties, and functions that render a privacy scheme or model distinguishable and unique from other schemes or models. The significance of adopting abnormal design features is very valuable. It offers the aspect of uniqueness and distinguishability to ease the work for the field researchers [123].

3.2.16. Security achievements

It can be referred to as the security outcomes or accomplishments of certain functions of the security system. Security achievements provide the final results and capabilities of the security systems, such as the security level achieved after implementing a specific algorithm, obtaining results about what type of security attacks addressed, and provide a security evaluation report to point out critical elements that affect the final security results [124].

CHAPTER 4

THE COMPARISON OF PRIVACY-PRESERVING SCHEMES FOR THE CLOUD STORAGE

4.1. Introduction

The need to process and store data of great sizes has increased enormously with the development and the emergence of new notations in the fields of Internet and informatics. Besides, the maturity of cloud computing has contributed effectively to the management of electronic data and removed all obstacles and difficulties faced earlier by cloud service clients and data collectors. But the significant advancement in the cloud computing sector comes with a huge cost. Security and privacy problems started to escalate and got more complicated due to the huge demand and high usage of cloud computing services. According to Microsoft reports, A huge deviation occurred in the use of cloud services due to global catastrophic events and social distancing [125]. However, the overwhelming presence of security and privacy threats began to nibble and weaken a cloud computing structure. Field researchers have awakened to the fact that these threats need to be addressed as soon as possible and no matter the cost.

Although many attempts have been considered to address security and privacy attacks, such as access control solutions, cryptographic solutions, and secure cloud database solutions, there are many security and privacy gaps that need to be covered. It is important to mention that across the last decade, many research papers have been written over the security of cloud computing with suggested and novel countermeasures to address security and privacy attacks on the cloud environment [126], [127], [128]. Even though, with all the solutions and countermeasures proposed to sort out the dilemma of security concerns in the cloud, only a few of these models

were capable of enhancing the security characteristics of the cloud environment. A handful of suggestions have been projected to formulate a comparison of the state-of-the-art study about security and privacy countermeasures to understand better and help future researchers discriminate and find more appropriate solutions between the category of security models. In this chapter, we will conduct a comparison study on privacy-preserving models directed only to protect cloud storage structure. We will adopt eight different privacy-preserving schemes, which is the ideal number of models to conduct a comparison study. But first, a brief description will be made about the methodologies of gathering resources in terms of the privacy-preserving schemes and privacy attributes, and the idea behind selecting each privacy-preserving schemes and privacy attributes. At the end of the chapter, we will answer the research hypotheses formulated earlier to reach the maturity of our research by addressing the problems and solutions, which in turn result in an optimal security medium for cloud storage.

4.2 The choice of privacy-preserving schemes and privacy attributes

4.2.1 How privacy-preserving techniques are chosen?

Throughout our study and observation of the literature, we managed to discover creative and novel schemes with unique security properties. We focused the efforts on utilizing seven security schemes, including an access control scheme, secure data sharing scheme, Secure cloud storage scheme, integrity check scheme, data hiding scheme, confidentiality auditing scheme, secure cloud-database scheme. We managed to analyze these schemes independently to search for common privacy attributes that can be implemented in the comparative study. The selection of these approaches has been built upon several key steps:

- **A comprehensive and unique selection**

  In our study, we tried to combine conceptual and mathematical approaches through the search for flexible, rich with security features, and lesser complex approaches [19]. However, we could have tried to select more than seven approaches to conducting our comparison study, but it will be too

complex and time-consuming to extract common privacy attributes. Where most of the privacy-preserving approaches around the internet either have a high level of complexity or does not describe the case properly [129], [130], [131]. Also, we attempted to cover most of the important approaches that uniquely adopt the privacy-preserving concept. However, the lack of enough resources will create irregularity and fault-tolerant in the comparative study. Accordingly, we decided to adopt only seven approaches to create a scientific balance between time and comprehensiveness to evaluate most of the approaches with lesser effort.

- **Common privacy attributes**

  The selection of privacy-preserving techniques is driven by the distinct presence of the common attributes. These privacy attributes allowed us to distinguish between various privacy and security approaches so that the selection depends on the level of occurrence of these attributes in the structure of privacy and security approaches.

- **Level of complexity**

  Although privacy schemes can be founded everywhere on the internet, there are several schemes that contain complex mathematical representations, which could be a formidable task to interpret and transmit into a simpler and understandable form [132], [133]. In this study, we tried to find privacy schemes with a lesser level of complexity and resourceful enough to extract the common attributes.

Although each scheme has a different approach to secure cloud storage, all schemes aim to address a dangerous type of attacks on cloud storage with promising results of achieving the optimal privacy-preserving solution:

1. **Sheren et al. scheme (Access control scheme)**

   Access control gives the required capabilities to the designer of the security system to enhance the confidentiality level of cloud storage by delivering a preventative measure against many types of trespassing [134].

This scheme introduces an advanced multi-authentication system to prevent unauthorized access to cloud data. Also, this scheme contains the major infrastructure for a pure privacy-preserving system.

2. **Yuan et al. scheme (Secure data sharing scheme)**

Secure data sharing systems encourage different parties to share data safely with the presence of a flexible and accountable cryptographic system [135]. This scheme provides a special algorithm called Path-ORAM that shaped the cloud storage structure with refined features that increase security efficiency. In addition, an identity-based signature accompanied by symmetric encryption system is implemented to strengthen the security of the scheme and introduces privacy assurance for cloud storage.

3. **Ganapathy, S. et al. scheme (Secure cloud storage)**

Securing cloud storage has become a vital matter when we talk about cloud computing. It has been proven that ensuring cloud storage security is highly recommended due to the huge demand from IT experts for cloud storage service [136], [137]. From our perspective, we took this scheme because it has the potentials to preserve user and data privacy due to the substantial design of the cryptographic system. The use of the CRT algorithm (Chinese remainder theorem) with the key-management system made the expectations high of ensuring the confidentiality of valuable information held in the cloud storage.

4. **T. Subha et al. scheme (Integrity checking scheme)**

Integrity checking systems create a popular solution in terms of protecting data privacy. While Integrity checking systems must fulfill three essential aspects, including correctness, completeness, and freshness, that results in a secure and reliable system [138]. The selection of this scheme relied on the improved design of an anti-tampering scheme [139], which in turn prevents the alteration attempts on data transmitted between parties. This scheme can discover the source of the transmitted data and investigate its reliability and legality.

5. **Yu Jin et al. scheme (Data anonymization scheme)**

Data hiding techniques built the foundation of data security by involving new approaches such as [140], [141] to conceal special and important data away from suspicious and untrusted parties. We choose this scheme based on the level of novelty it possesses in terms of methodology, design, and results. Yu Jin et al. scheme introduces a unique scheme that uses the Lagrange interpolation method to hide data and secure cloud storage. In addition, it uses a multi-cloud structure, which is the proper solution to address data privacy concerns. It also provides the feature of service availability to overcome the challenges of system failure.

6. **Zhen Yang et al. scheme (Confidentiality auditing scheme)**

Confidentiality auditing offers possibilities and trustworthy systems that encourage users to store their data on the cloud by inspecting the transmitted data between users and CSP [142]. The unique capabilities and rare characteristics packed in this scheme, such as the authentication model based on the use of users' aliases for privacy-preserving assurance and the use of public auditing system, resulted in a scheme that can conceal sensitive data from potential security violations.

7. **Liu Guoxiu et al. scheme (Secure cloud database scheme)**

Cloud database services emerged as a role-player element in cloud computing. The huge demand for a service which has the characteristics of affordability, flexibility, and efficiency made cloud database service one of the highly used cloud service [143]. Liu Guoxiu et al. scheme offers a novel triple encryption system to secure cloud storage, making this scheme a suitable candidate for our comparative study. This scheme presents a methodology that can calculate and process any type of digital data without compromising its security and satisfy the requirements needed to attain a privacy-preserving system.

4.2.2 How common privacy attributes are chosen?

We have observed recent literature studies on cloud security and its attributes that formulate the optimal security and privacy solutions for cloud environments [144]. These attributes have been chosen based on the detailed analysis of privacy-preserving approaches. In our selection, we took into consideration the strong relationship between privacy and security of the cloud storage and each independent attribute. We also noticed that these attributes are shared between our group of privacy-preserving approaches, which made these attributes the perfect candidates for the comparative scenario. The following subsequent sections will briefly demonstrate the idea behind the selection of each privacy attribute:

- **Data Auditing approaches**

  It has been observed that data auditing help maintain a stable level of performance and security in the cloud environment. Many studies refer to cloud data auditing as the tool for assessing risks and predicting the threats before it hit the system [145]. In contrast, others refer to data auditing as the method for creating an appropriate and cost-effective work environment [146].

- **Cryptographic techniques**

  A safe and reliable environment is what cloud users need to access shared data without the concerns of security and privacy violations. Cryptographic techniques are considered the best approaches to secure cloud data through the process of encrypting high-value data. Cryptographic techniques guarantee the reliability of important data that reside in cloud storage and ensures the most secure data-sharing environment [147].

- **External assets**

  Various implementations in privacy-preserving schemes have proven to be an effective asset in terms of presenting new methodologies and capabilities. Adding special assists such as algorithms, mathematical representations, and formulas to the privacy-preserving system help in solving design obstacles and at the same time strengthens the underlying security structure of the system.

- **Key generation techniques**

  Key generation techniques are essential in the design of cloud security countermeasures. Secure systems must have unique key generation techniques, which can resist many attacks and can forge the most complex keys to keep encrypted data safe against potential danger [148].

- **Key length**

  Most of the secure systems use large key length (key size) to maintain the security of high-value data. It is important to mention that key length is an essential feature of designing security systems and achieving a certain amount of confidentiality [149]. However, designers must be seriously careful when choosing key lengths because their designs' security depends on the degree of complexity to crack the key.

- **Key management**

  The importance of a key management system lies with investing in an exceptional administration system for encryption keys. Such an attribute can affect security in a positive way to create the most secure and reliable system to use in the cloud environment [150].

- **Key function**

  Understanding the roles of the encryption key have a great necessity when it comes to the design of security systems because encryption keys have several functions such as encryption, authentication, verification, and digital signature, which is a mandatory aspect to comprehend by field experts [151].

- **Design features**

  Smaller pieces in the design of cloud security countermeasures have a great influence on the environment in which it will be applied, where fresh designs should focus on implementing security and agility features across all the layers of cloud infrastructure [152].

- **Performance standards**

  Performance evaluation is considered one of the most important elements that can determine the capabilities offered by cloud security countermeasures. However, performance evaluation and criteria should target the base elements of cloud security countermeasures to introduce more possibilities for future improvements [153].

- **Threats type**

  It is important to mention that various privacy-preserving systems are most likely vulnerable to different types of security and privacy attacks. Determining the type of security or privacy peril is important, especially at early stages in security system development or even post-launch. Early detection of such threats is something valuable for most of the systems, and it will decrease or even eliminate the danger that may face the security systems when it functions in vulnerable environments.

- **Threats addressed**

  The main objective of privacy-preserving schemes is to eliminate the danger surrounding cloud storage service. Addressing serious security and privacy violations has a great influence on gaining user's trust and ensuring the obligation to the security and privacy standards [154].

- **Test environment**

  Privacy-preserving schemes require an evaluation and a test environment to study the performance and behavior of the fresh schemes. The importance of the test environment lies in its ability to simulate the regular cloud environment and examine the outcomes of the scheme based on the performance standards made by the designers. The unique nature of the cloud environment can create a proper sphere to conduct the security and performance tests over privacy-preserving schemes [155].

- **Tests applied**

  A variety of special and objective tests are conducted to evaluate privacy-preserving systems. Evaluation tests prove to be an effective attribute to specify the number and type of experimental tests. These kinds of tests help designers of privacy systems to inspect and measure the strengths and weaknesses of every function in the privacy-preserving scheme.

- **Cloud-storage structure**

  The representation of cloud storage is uniquely important in designing security and privacy countermeasures for the cloud environment. It is mandatory to focus the efforts on adopting new cloud storage structures, such as multi-cloud storage, which can ease the development of efficient, flexible, and accountable security systems [119].

- **Abnormality**

  Most privacy-preserving techniques have the same goal of protecting the privacy of user's data. However, each privacy scheme has its own way of delivering security and privacy aspects. We managed to add an abnormality attribute (Exceptions) to our comparison, which shows a promising result in terms of distinguishing between privacy schemes by function, features, performance, and capabilities [123].

- **Security achievements**

  It is important to mention the security achievements as one of the unique privacy attributes. Security achievements show the strengths of privacy-preserving schemes by presenting the factors contributing to the defense against security and privacy attacks.

4.3. The comparative scenario

In this section, we will conduct a comparative study for seven privacy-preserving schemes of cloud storage. The comparison will use various common/privacy attributes as evaluation parameters to find the strengths and

weaknesses of each privacy-preserving scheme's structure. Comparison results will be reviewed and organized as an evaluation tool to help future researchers comprehend the idea of privacy countermeasures in the cloud environment:

4.3.1 Matrix of the comparison result

Table 4.1 Matrix of the comparison results of privacy-preserving schemes

Common privacy attributes	Sheren et al.	Yuan et al.	Ganapathy, S. et al.	T. Subha et al.	Yu Jin et al.	Zhen Yang et al.	Liu Guoxiu et al.
Data Auditing approaches	Third-party auditor	Internal Auditing	Internal Auditing	Third-party auditor	Internal Auditing	Third-party auditor	(Internal Auditing
Cryptographic techniques	Advanced encryption standard and Hash function with Shared secret key	Symmetric encryption using Counter mode (CTR) of the Advanced encryption standard and Elgmal algorithm for	CRTSSA (a combination of Caesar cipher technique and encryption formula)	Public-key technique, digital signature, and certificates	Not mentioned	Broadcast encryption, Hash function, SHA-1	Randomized encryption and AES with ECB, Monotonic encryption model, and Homomorphic encryption model

		public-key encryption					
External assets	RFC (6238) One-time password algorithm	Identity-based signature scheme	Chinese remainder theorem	Not mentioned	Lagrange Interpolation algorithm	Not mentioned	The implementation of non-linear order-preserving indexes algorithm and special cryptosystem which help deal with SQL queries

Key Generation techniques	KEYGEN algorithm for creating public and secret keys	IGen for creating the signing keys, SGen for symmetric key generation, and PGen for public key generation	A newly proposed algorithm called CRTKGA for generating encryption and decryption keys	Public and private keys generated by the data owner	Not mentioned	Public-key encryption technique is used to generate a pair of public and private keys	Proposed formula for generating encryption/decryption keys
Key length	Random key-length	Random key-length	56-bit, 128-bit, 512-bit, 1024-bit	Random key-length	Not mentioned	Random-key length	Random-key length
Key management	Not mentioned	Not mentioned	Group key-management system	Not mentioned	Not mentioned	Not mentioned	Master and session key management system

Key functions	Encryption, Decryption, and Digital signature	Encryption, Decryption, Digital signature	Encryption, Decryption	Encryption, Decryption, Digital signature, Verification	Not mentioned	Encryption, Decryption, Digital signature, Verification	Encryption and Decryption
Design features	The use of OTP to authenticate and certify cloud users. And the use of automatic blocker protocol to authenticate and certify TPA.	Special storage structure that shaped as binary-tree, special data block format that consists of two parts the address of data block and the data itself	System structure contains UI, cloud database, data collection module, decision manager, and secured data storage	The client-side has three design activities, including Init. Phase, Key-gen phase, and Tag-gen phase. While TPA and CSP are responsible for two design activities, includi	The implementation of Lagrange interpolation to function as an encryption tool, and deployment of cloud server on four cloud service providers	The use of hashed client aliases to ensure the privacy of user's data. Also, the scheme involves using Confidentiality-based certificates to achieve data confidentiality with the help of security and privacy features	This scheme uses SQL queries and operations. This system also presents a triple-encryption system to hand cryptography processes to store different types of digital data inside cloud storage.

				ng the challenge-response phase and Proof verification phase			
Performance standards	Average request time and Throughput	The amortized cost, average execution time per operation for block and storage, and average communication cost	Encryption/ Decryption time analysis, Key computation time analysis, Key recovery time analysis, and security level analysis	Communication cost compared to the number of blocks, Auditing time compared to the number of blocks, privacy	Data level of confidentiality, time consumption during upload/ download operations, and storage space	Time cost for initialization and setup, Inspection performance, and Inspection cost	Execution time for the triple-encryption system, execution time between the proposed scheme and other database schemes, processing cost, and

				preservation performance			storage space between the proposed scheme and CryptDB
Threats type	Passive and active attacks	Active attacks	Active attacks	Active attacks	Active attacks	Active attacks	Active attacks
Threats addressed	Man-in-the-middle attack, a known-plaintext attack	Access patterns and message modification attacks	Replay attacks and message modification attacks	Man-in-the-middle attack, modification, and altering of message contents	Denial of service and message modifications	Access patterns, Man-in-the-middle, message modification	Cipher-text only attack and chosen-plaintext attack

Test Environments	Programming language: Java for developing the scheme Cloud environment: Tomcat virtual server with the penetration test application called OWASP	Programming language: C++ OS: Ubuntu 16.04PC Hardware: Core I5 with 4GB of Random-access memory	Programming language: Java OS: Window 2008 Cloud environment: CloudSim with Eclipse	OS: Centos 6 Hardware: I5 3520, 500GB HDD, 8GB of Random-access memory Cloud environment: Eucalyptus as a private cloud server	Programming language: Java User interface: SWT Cloud environment: Cassandra databases	Client hardware: Intel Celeron N3050 CPU with 2GB of random-access memory TPA hardware: Intel Core I5-5257U CPU with 8GB of random-access memory Cloud environment: Private Local area network	Programming language: Java OS: Centos Hardware: Intel Xeon CPU E3-1226 with 16GB of random-access memory

Tests applied	SQL injection, Corrupted and unauthorized access, Data exposure, Cross-site request forgery, and performance estimation tests	Zero-knowledge shuffle correctness proof, and additional performance evaluation tests	Performance and efficiency analysis tests	Performance and efficiency analysis test	Performance and efficiency analysis test	Data confidentiality test, user accountability test, privacy preservation test	Performance tests of encryption systems and evaluative test over web applications using SQL operations
Cloud storage structure	Single cloud environment	Single cloud environment	Single cloud environment	Single cloud environment	Multi-cloud environment	Multi-cloud environment	Single cloud environment

Abnormality	The implementation of Automatic blocker protocol, which secures and certify the third-party auditor	The use of a special cloud storage design called Path-ORAM, which reduced the cost required to establish a safe and reliable communication line	The use of CRT-based algorithms to design secure cloud data storage	The adoption of MHT which can authenticate data blocks	The use of mathematical representation to function as a cryptographic technique to achieve data hiding property	The unique design of Confidentiality-based certificates	The scheme uses an order-preserving algorithm to handle the indexes of data during the execution of SQL queries. It also provides some security features to help add another layer of defense to the proposed scheme

Security achievements	Eliminate the ability of TPA to expose sensitive data to the cloud service provider	Un-authorized users do not have the ability to perform any type of operations on cloud data. Also, the server cannot expose any sensitive information to the public with and without access patterns	Building secure cloud data storage with a high level of security properties ensures the confidentiality and integrity of cloud data.	The propose scheme protects data transmission between network participants against active adversaries	The assurance of data integrity and service availability	The assurance of achieving privacy preservation property and user accountability	Protection against different ways of revealing valuable data to unauthenticated entities

4.4. Answers to research hypotheses

- **What are the most important motivations that make individuals and organizations prioritize the privacy of information when outsourcing personal and sensitive data to the cloud environment?**

  The invention of new ways to handle information has had different types of influences on IT sectors. Cloud computing had its share from this implication in an effective and productive way. However, these types of advancements affect and weaken the security structure to become the unsolved mystery of this era. Privacy and security breaches on cloud vital and important data have proven to be the major concern of individuals, organizations, and even governments. Today, Privacy and security violations can introduce more vicious types of difficulties than ever before, and these problems must be addressed immediately and with the proper tools to protect high-value data [23].

- **How complex should the structure of a privacy-preserving scheme be to deliver an optimal security and privacy solution?**

  Usually, security systems use advanced and complex structures to shape the most effective and error-free solutions. However, complexity may not always deliver promising results. In fact, the complexity of privacy-preserving schemes can affect various types of functions and may negatively affect the overall performance of the entire system. Problems such as high computation time, access and maintenance difficulties, higher developing costs, and waste of system resources are usually founded in complex systems. The design of privacy-preserving schemes should be elastic, efficient, and reliable to lower the probability of encountering any security or performance challenges.

- **What is the impact of privacy/common attributes on the security and privacy aspects of the cloud environment?**

  Cloud computing has been considered as one of the dangerous zones for managing and processing data due to its ability to deliver an open environment

to use by different types of entities. However, privacy attributes invented to build and support a variety of privacy-preserving schemes for protecting users and data privacy. In contrast, the extraordinary nature of these attributes provides the adaptability feature for privacy-preserving schemes to stand against distinctive forms of cyber threats. The impact of privacy attributes has been observed through many experimental tests; for example, cryptographic techniques have the security tools and properties to process different data types and convert them to encrypted representation, which can only be accessed by authenticated and authorized individuals [24].

- **Is it possible to build mutual trust between data owners, users, and cloud service providers regarding information and data privacy?**

  Security and privacy aspects use the principle of trust as an estimation tool to measure the level of authenticity and reliability of the desired entity. In the cloud, trust plays a significant role in securing connections established between system participants. In fact, we can only consider the data owner as a trustworthy entity in the cloud network because data owners cannot exploit their private data and jeopardize sensitive information to a variety of security and privacy intrusions. While other participants, such as cloud users and CSP (cloud service provider), may have the curiosity to have some knowledge about the data transmitted through the cloud network. Nowadays, most cloud service providers are growing towards increasing clients' trust by offering substantial security and privacy features that can encourage new clients to use their services.

CHAPTER 5

RESULTS AND DISCUSSION OF PRIVACY ATTRIBUTES

5.1. Results analysis of common privacy attributes

5.1.1 Data auditing approach

Data auditing offers new ways to establish the best possible work environment by addressing various challenges, such as data security and data integrity. According to our comparison table in chapter 4, Sheren et al., T.Subha et al., and Zhen Yang et al. schemes used a trusted third-party auditor as an inspection tool to examine and oversee all the transmitted data between data owners or cloud users and CSP. However, the third-party auditor's control over communications in the cloud network raises a new level of security and privacy concerns. The third-party auditor's untrusted nature may raise a significant probability that the third-party auditor is responsible for these critical concerns. On the other hand, Yuan et al., Ganapathy, S. et al., Yu Jin et al., and Liu Guoxiu et al. adopted an internal data auditing approach, in which the internal participants are the responsible authority for inspecting data integrity. However, using internal auditing may cost many resources as data owners or cloud users may not be able to inspect and evaluate certain activities in the cloud network.

5.1.2. Cryptographic techniques

Cryptographic techniques allow data owners to establish a ground-based role for their valuable information. Encryption techniques grant the capability to transform traditional types of data into more complex representations. Our comparison results show that all schemes involved in the comparative study used dissimilar types of cryptographic techniques except for Yu Jin et al. scheme, which uses a mathematical representation called Lagrange interpolation to hide and secure data contents. In

Sheren et al. scheme, the idea of using two types of encryption is that one of them will be assigned to encrypt the user's data, and the other one is the hash function with a shared secret for encrypting the OTP function. Likewise, Yuan et al. used two types of encryption techniques the Counter mode of Advanced encryption standard for encrypting user's data and the Elgmal algorithm to encrypt the public key and provides the security properties for encryption keys. Ganapathy, S. et al. scheme employed a proposed algorithm called CRTSSA that consists of two layers of encryption, including Caesar cipher encryption technique and proposed encryption formula to secure cloud data storage. T. Subha, in his scheme, utilizes a public key algorithm as the main encryption tool and digital signatures along with certificates to provide the means of authenticity and data integrity. Furthermore, Zhen Yang et al. adopts a mix of several encryption schemes, including broadcast encryption to encrypt data and perform key distribution, Hash function to create a hash identifier for each user in the network, and SHA-1 to convert user identifiers to random identifiers to create some kind of confusion for adversaries. Also, Liu Guoxiu et al. implement a unique triple-encryption system that consists of three layers of encryption. The first layer combines a randomized encryption technique with the Advanced encryption standard that uses the Electronic codebook to encrypt SQL queries. The second layer is called the monotonic encryption system to encrypt numerical data types without touching the order of data content and with the support of range queries. The last layer uses Homomorphic encryption to encrypt numerical data, but it differs from the previous layer by only supporting addition and multiplication queries.

5.1.3. External assets

The external algorithms added to the privacy-preserving techniques have driven the security system's design to a whole new level. External algorithms such as RFC (6238) for one-time-password that has been used by Sheren et al. scheme present security countermeasures that can address access control attacks. Yuan et al. apply an Identity-based signature scheme to generate digital signatures, which can be used to authenticate cloud users. Also, Ganapathy, S. et al. adopted the Chinese remainder

theorem to formulate encryption and key generation algorithms. Likewise, Yu Jin et al. utilize mathematical representation called the Lagrange interpolation to construct security properties such as data hiding and data confidentiality within his scheme's structure. On the other hand, Liu Guoxiu et al. conduct a special technique called the Monotonic encryption scheme. This scheme offered an exceptional feature to encrypt numerical representation of digital data and at the same time preserve the order in which data contents are organized.

5.1.4. Key generation techniques

Like cryptographic techniques, diverse types of key generation algorithms have been used by the privacy-preserving schemes. Due to the efficiency and reliability of the public-key cryptography technique, Sheren et al., Yuan et al., T. Subha et al., and Zhen Yang et al. used this algorithm as a common key generation technique to generate pair of public and private encryption keys. However, Yuan et al. preferred to use additional algorithms, including IGEN, for creating signature keys to add a bit of authenticity to the scheme along with the symmetric key generation technique. While Ganapathy, S. et al., and Liu Guoxiu et al. apply proposed algorithms and formulas to produce encryption and decryption keys. On the other hand, Yu Jin et al. scheme was the only scheme that does not integrate the key generation technique because of the presence of a mathematical algorithm.

5.1.5. Key Length

For the key length, Sheren et al., Yuan et al., T. Subha et al., Zhen Yang et al., and Liu Guoxiu et al. schemes used a random key length for their cryptographic operations inside the scheme. Using a random key as an encryption key is very fruitful in terms of building highly secure systems. While Ganapathy, S et al. scheme used different key lengths to encrypt data, including 56, 128, 512, and 1024-bits. On the other hand, encryption keys are not used in the design of the Yu Jin et al. privacy-preserving scheme.

5.1.6. Key Management

The key management system in Sheren et al., Yuan et al., T. Subha et al., Yu Jin et al., and Zhen Yang et al. scheme is not supported. While Ganapathy, S et al. scheme applied the group key management system to manage encryption keys and restrict the delivery of these keys to authorized users only.

5.1.7. Key function

As for Key function, Sheren et al. scheme used a single key function, the digital signature, to prevent the encryption key's reforming and ensure authentication and data integrity. Also, Ganapathy, S et al., and Liu Guoxiu et al. used encryption only as a key function to encrypt outsourced data. However, Yuan et al., T. Subha et al., and Zhen Yang et al. schemes used multiple key functions to achieve data confidentiality, data integrity, and data verification.

5.1.8. Design features

Design features play a vital role in any comparative study. Sheren et al. adopted an OTP-based system that uses a mobile application to generate temporary codes to authenticate cloud users. In addition, this scheme used an automatic blocker protocol to function as a verification tool. This tool verifies the third-party auditors' authenticity to prevent any unauthorized attempts to masquerade or manipulate cloud data. Yuan et al. apply a special design for his scheme by employing the Path-ORAM algorithm in which data blocks are represented as a binary tree. Besides, Yuan uses a phenomenal data block structure in which block address and data content are the main parts of the data block. Also, Ganapathy, S et al. import unique design that consists of several components including User Interface for client interactions and activities, cloud database for data storage, data collection module for responding clients' requests, decision manager to control system functionalities, and data storage for encrypting and decrypting data transmitted throughout the system. T. Subha et al. implement a design feature that considers two unique stages. Client stage, in which several processes are executed over the plain data, including data segmentation, encryption/decryption key

generation, and signature generation. While data auditing stage, in which data are inspected and verified to formulate a test report that proves the authenticity and integrity of the transmitted data. Yu Jin et al. design an unusual privacy-preserving scheme in which numerical analysis formula called Lagrange interpolation is used to build the scheme body. Yu Jin used the Lagrange formula to encrypt plain data blocks and hide them by using two essential parameters the data blocks themselves and points on the x-axis, which in turn can construct the interpolation polynomial. In addition, Yu Jin used a multi-cloud storage structure in which encrypted data blocks are split between the number of cloud servers to eliminate the problems that impact service availability. Furthermore, Zhen Yang et al. utilizes an incredible feature to hide users' identities by generating a hash identifier for each cloud user. Also, he formulates a special type of certificates to function as proof of confidentiality to the third-party auditor. Finally, Liu Guoxiu et al. employ SQL queries to transmit data through a cloud network instead of simple representation. This feature helped with encrypting different types of data with less impact on data security. Also, Liu Guoxiu et al. scheme used a triple-encryption system that encrypts different types of data representations through three types of encryption techniques to achieve data confidentiality and accountability.

5.1.9. Performance standards

There is a significant divergence in the performance standards that have been used in the privacy-preserving schemes. For example, Sheren et al. conducted two types of performance standards to evaluate her scheme. Average request and response time versus the number of cloud users to measure the amount of time needed to send and receive the one-time codes. And the throughput of the proposed scheme versus the number of current users. Yuan et al. took into consideration three parameters to measure the performance and efficiency of his scheme, including amortized cost, the average execution time for each operation applied versus both storage and block sizes, and average communication cost for both read and write operations. While Ganapathy, S et al. used several parameters, including encryption/decryption time analysis, key computation time analysis, key recovery time analysis, and security level analysis as

an evaluation standard to measure the performance between the proposed scheme and other traditional algorithms such as AES and DES. T. Subha et al. allocates three performance measuring parameters, including communication cost versus the number of blocks during auditing operation in which a transmission of data has occurred, auditing time versus the number of blocks, and privacy-preservation performance during active attacks. Yu Jin et al. used three parameters to assess the performance of the entire system. Data level of confidentiality shows results about the level of data confidentiality between the Yu Jin scheme and another scheme that uses AES as an encryption technique. Time consumption for download/upload is another parameter that measures the time needed to complete the full download/upload process for the proposed scheme compared to other traditional schemes. In terms of storage space, this parameter measures the amount of storage needed during scheme execution between the proposed scheme and other schemes. Also, Zhen Yang et al. rely on three types of parameters including time cost for initialization and set up to measure the time required for preparing the main functions of the scheme, inspection performance for benchmarking the capabilities of the auditing mechanism, and inspection cost to calculate the cost required by auditing tool to complete full auditing process. Finally, Liu Guoxiu et al. employed a variety of performance standards to cover the evaluation process of his scheme. The execution time of the triple encryption system to calculate the amount of time needed to encrypt one SQL query. While the execution time of the proposed scheme versus another database scheme also calculates the time required to finish full execution of certain action between two different database schemes. Lastly, processing cost and storage space are other parameters to measure cost-effectiveness and the amount of storage required between the proposed scheme and the CryptDB scheme.

5.1.11. Threats type

Regarding the types of security and privacy attacks, our comparison results show that active attacks are the main reason behind these security and privacy

violations. While Sheren et al. scheme results show that her scheme is also addressing other problems caused by passive attacks.

5.1.12. Threats addressed

Privacy-preserving schemes have addressed different forms of security and privacy attacks. Most of the privacy-preserving schemes have a common type of attack that is addressed by running scheme algorithm. However, there are additional security and privacy attacks that have also been addressed. Sheren et al. scheme focused on solving the challenges of Man-in-the-middle and Known plain-text attacks because of its nature that brings TPA as an additional party, which might endanger the whole network's security. Yuan et al. scheme has solved the problems caused by access pattern and message modification attacks, which might be caused by several activities done by malicious users. Ganapathy, S et al. scheme managed to overcome the difficulties that emerged from Replay and message modification attacks by eliminating the means of unauthorized access to cloud storage. T. Subha et al. scheme explained and tackled Man-in-the-middle and message alteration attacks by using a special type of digital signatures and certificates. The denial of service and data modification attacks were the biggest concerns for Yu Jin et al. scheme. Yu Jin implemented a mathematical scheme called Lagrange interpolation to create a privacy-preserving solution by introducing several properties such as data hiding and service availability. Also, Zhen Yang et al. have encountered multiple attacks on the security and privacy of cloud storage, including access control attacks, Man-in-the-middle attacks, and message modification attacks. However, he managed to resolve these issues by adopting a unique feature called users' identifiers that proved to be an effective tool against the attacks mentioned earlier. Finally, Liu Guoxiu et al. create a phenomenal database scheme that presented a solution for two types of adversary attacks, including cipher-text only and chosen-plaintext attacks.

5.1.13. Test environments

Most of the privacy-preserving schemes mentioned in the comparison used Java as the main programming language to develop their schemes. The compatibility and efficiency of Java with various types of hardware and test environments make it unique and widespread throughout the world. However, Yuan et al. scheme used a different type of development platform, which is C++. Also, various test hardware has been used for each type of privacy-preserving scheme with respect to the functionality and processing required by each scheme. Yet, the efficiency of each scheme relay on test hardware capabilities, for example, a privacy scheme that works on a machine with Intel Core I7 and 16 GB of Ram is more productive and efficient than a machine that runs with Core I5 and 8 GB of Random-access memory, and the same situation goes for the operating system.

5.1.14 Tests applied

Performance and efficiency tests have taken the highest priority because of the significant importance it possesses in the privacy-preserving scheme. In fact, most of our comparison schemes took the traditional performance and efficiency tests as evaluation criteria to measure how effective the schemes will be after the deployment in the cloud environment. However, Sheren et al. conducted additional tests, including SQL injection, broken authentication and session management, data exposure, cross-site request forgery, and bad traffic to compare with previous privacy-preserving schemes results. Yuan et al. use a special test called Zero-knowledge shuffle correctness proof to prevent malicious adversaries' data tampering. While Ganapathy, S et al., T. Subha et al., and Yu Jin et a. utilized the traditional tests, including performance measuring based on cost, time, and storage, and experimental analysis to system functionalities. On the other hand, Zhen Yang et al. perform several tests over his scheme, including a data confidentiality test to assess whether data is transmitting safely between cloud entity without modification or theft attempt, a user accountability test to check if cloud users are trustworthy or not, and privacy-preserving test to check

whether the third-party auditor is leaking information or not. Finally, Liu Guoxiu et al. employed a performance test over the triple-encryption system to calculate the average time needed to execute SQL queries. Also, he tested the compatibility of the scheme with web applications (third-party database applications) using SQL operations to calculate the average execution time in these types of applications.

5.1.15. Cloud storage structure

Most of our comparison schemes have considered using a single cloud structure as a cloud storage environment. Single cloud structure offers unique capabilities such as full control over cloud servers with high privileges and a huge amount of separation from other cloud servers, which benefit security and privacy aspects. On the other hand, Yu Jin et al. and Zhen Yang et al. schemes adopt another concept that is becoming popular these days called multi-cloud structure. Multi-cloud storage structure also has advantages, including cost-efficient, better allocation of cloud servers around the world, powerful processing environment, and risk management.

5.1.16. Abnormality

Exceptional behavior and characteristics create a significant impact on the overall performance of the privacy-preserving schemes. Sheren et al. implemented a unique feature that affects the security aspect of the scheme. She introduces an Automatic blocker protocol that prevents unauthorized access attempts from accessing private data by issuing a stop operation to the auditing protocols located within the third-party auditor. Yuan et al., in his scheme, enhanced a design of ORAM-based scheme by importing a special design for cloud storage called Path-ORAM that transforms the traditional cloud storage structure with a binary tree shape. This methodology has proven to be cost-effective in terms of communications between cloud parties. Ganapathy, S et al. implemented the Chinese remainder theorem in his design of a privacy-preserving and secure storage scheme. The CRT formula has been used in the encryption and key generation algorithms to enhance the scheme's security

characteristics. T. Subha et al. adopted a hash-based data structure called the Merkle hash tree. T. Subha used the Merkle hash tree as an authentication tool to find the corrupted data blocks and separate them from reliable and attested ones. As we mentioned earlier, an exceptional formula called Lagrange interpolation is used by Yu Jin et al. scheme to operate as a cryptographic technique that hides data blocks and at the same time fulfills both data confidentiality and service availability properties. In contrast, Zhen Yang et al. utilized a novel design for confidentiality-based certificates, which serves as proof for the auditing party. These certificates help the third-party auditor to distinguish between authorized and unauthorized access to cloud data. Finally, Liu Guoxiu et al. recall an earlier method to keep the order of data indexes as formal as possible after each encryption process. It also allows SQL operation to be executed directly over encrypted data without raising any security or privacy concerns.

5.1.17 Security achievements

The aim of designing privacy-preserving schemes is to integrate security and privacy aspects within the security systems structure and produce a specific number of security achievements. In Sheren et al. scheme, the security goal is to prevent the third-party auditor from endangering sensitive and vital data during the auditing process by exposing data contents to other entities in the cloud network. While Yuan et al. scheme yield several security outcomes, including the preventability of unauthorized users to manipulate or alter cloud data, and the third-party auditor cannot reveal high-value data to the public either with or without access patterns. The dual encryption and key generation approach of Ganapathy, S et al. scheme resulted in a secure and reliable cloud storage environment with the introduction of multiple security and privacy properties, including data confidentiality and data integrity. Also, T. Subha et al. scheme reaches the maturity of the security concept by utilizing digital signatures and certificates, which provides the authenticity and reliability of the transmitted data. The use of a data hiding approach such as Lagrange interpolation and the use of multi-cloud storage structure in Yu Jin et al. scheme resulted in two main security achievements, including the assurance of data integrity and service availability.

Whereas Zhen Yang et al. scheme accomplishes both privacy-preservation and user accountability goals by designing a unique version of cryptographic certificates. Lastly, Liu Guoxiu et al. scheme concludes promising results in terms of the protection of data privacy. The triple-encryption system allows for better security measures against several attempts to reveal critical information and data about specific cloud users.

5.2. Results summary of the advantages and limitations of the privacy-preserving techniques for the cloud storage

Table 5.1 The advantages and limitations of the privacy-preserving techniques for the cloud storage

Privacy preserving technique	Advantages	Limitations
Sheren et.al	The use of OTP authentication algorithm for users and Automatic blocker authentication protocol for auditing mechanism	The use of curious Third-Party Auditing instead of Internal Auditing and cryptographic techniques limited accountability
Yuan et.al	The scheme addresses the problem of access patterns for all system participants, along with achieving better performance than other ORAM schemes.	Significant effort required from users to store/access specific data blocks

Ganapathy, S. et.al	The implementation of CRT-based algorithms for encryption, decryption, key generation, and key management builds a secure interaction with CS.	Computationally complex and the use of familiar key sizes (due to the restrictions of the cryptographic techniques may create a challenge in achieving a certain level of security.
T. Subha et.al	Merkle Hash-tree is used to authenticate data blocks and eliminate the Man-in-the-middle threat.	The use of Third-Party Auditing that can expose the data to other threats instead of using Internal Auditing, which is securer and more reliable
Yu Jin et.al	Ensuring both data confidentiality and service availability by using Lagrange interpolation and Multi-cloud storage	If the adversary can obtain more than two data blocks, he can expose the original data because he can construct the interpolation polynomial
Zhen Yang et.al	Hashed client aliases and confidentiality-based certificates improve data confidentiality and auditing efficiency without introducing additional privacy risks	An Increase in the communication cost when using third-party auditing

Liu G. et.al	Layered encryption system that can support encryption of float numbers, SQL queries can be processed over encrypted data, and reduce computation overhead	Increase in the computational cost and space overhead. Also, performance test over a cryptographic system is not efficient.

5.3. Privacy attributes that have not been addressed in cloud security research

5.3.1. Scalability

Scalability can be defined as an entity's ability to extend or enlarge another entity's capabilities due to the massive demand for specific features or the lack of required resources to perform a particular process. In terms of cloud computing, Scalability plays a considerable role in IT industries when there is a shortage of cloud server resources to cover all the clients' requests. Scalability in cloud computing offers unique solutions for increasing cloud servers' capabilities, such as extending cloud storage limit, increasing the processing power with the implementation of parallel processing, and expanding the network bandwidth or cloud network coverage [156]. While there are several ways introduced in [157] to adopt the scalability feature for the cloud computing services, including IaaS (horizontal and vertical scalability), which can be represented in increasing the number of virtual servers or adding load balancers. And PaaS scalability, which can be adopted by increasing the number of container and database replicas.

Unfortunately, security and privacy violations have taken a critical role in the world of cloud computing, and the use of the scalability feature might be inefficient or harmful [158]. However, the introduction of several privacy-preserving and security

approaches made the use of scalability in the cloud environment feasible. Although, many privacy-preserving techniques have been introduced without turning any attention towards the significance of implementing the scalability feature. According to The Wall Street (an American journal) [159], Amazon.inc, Google, and Microsoft have witnessed an enormous increase in the use of their data storage and processing services because of the pandemic of the Coronavirus. These corporations have left the heavy burden of processing and storing data from Internet users by building a universal service infrastructure that connects people with their daily work using the Internet and cloud computing services [160].

The development in the cloud security sector, along with the noticeable increase in on-demand cloud services, encourages researchers to embrace the idea of scalability. Based on our knowledge, there are only a few privacy-preserving techniques that adopted the scalability feature in the design of the security system. Despite being an old scalability assurance technique, the HASBE (a hierarchical attribute-based solution) proposed and implemented in [161], [162] has all the unique constituents to establish a scalable privacy-preserving scheme that protects the cloud environment. The HASBE scheme relay on the use of a hierarchical system, which can, in turn, grant the permission of private key generation to lower authorities in the whole system that results in minimizing workload and increasing system efficiency. While the other technique that supports cloud scalability, which is called MapReduce, and it has been used in the same manner in several privacy-preserving techniques [160], [163], [164], [165]. The MapReduce framework aims to process and generate data of massive sizes by using symmetrical and distributed algorithms established on the computer nodes [166]. Both of the previously mentioned approaches provide the means to handle the problem of cloud security that keeps escalating day after another comprehensively and coherently.

5.4. Recommendations

Previous results include several vital points determining the best way to develop a secure and efficient privacy-preserving scheme for cloud storage. The design

of privacy-preserving schemes must be coherent and adaptable to withstand many security and privacy violations. It is highly recommended that privacy-preserving schemes must use internal auditing, which is more efficient and reliable than third-party auditors, which are usually untrusted parties and might put cloud networks under severe risks. In terms of cryptographic techniques, it is preferable to use asymmetric cryptographic methods that are more reliable and accountable than other methods, and it uses multiple keys to encrypt and decrypt data. It is also essential to encrypt sensitive and vital data at every stage in the system before outsourcing to cloud storage. The recursive encryption of important data will provide data confidentiality and prevent cloud service providers from manipulating personal data. External algorithms must not be complicated, which might trouble the overall performance of the whole scheme. While key generation techniques must be complex and use different algorithms to generate encryption/decryption keys. Privacy-preserving schemes must include key management systems because of the efficiency and flexibility it offers, such as secure space for keys, controlling the distribution of keys among cloud users, and updating the regulations and certificates. Key lengths must be relatively significant and random to prevent brute-force attacks and other forms of attacks on cryptographic keys. However, large and random keys may require much time to process and decrypt, but in the end, it can keep high-value data away from harm. Besides, privacy-preserving schemes must use various types of key functions to ensure optimal security by adding multiple ways to check the communications established inside the cloud network.

As for the design features, the designers of privacy-preserving techniques must implement the novel and the effective features and characteristics to enhance the scheme's main structure. Performance standards must be inclusive and objective to all functions inside the body of the scheme. For example, designers might need to consider the essential elements to measure inside their scheme, such as time, cost of development, storage space, privacy-preservation performance, and overall security achievements. Privacy and security threats must be studied and examined carefully to determine which type of attack put cloud storage in danger and which type of attacks

the scheme can address. This process requires a risk assessment for every kind of attack invented in the cyber world. The test environment must be elastic and compatible with the implemented scheme; this includes proper knowledge in different types of programming languages, the use of convenient software and hardware resources, and choosing the appropriate cloud server. Likewise, privacy-preserving designers must implement evaluation tests to assess the number of possibilities that can be provided by the scheme. Abnormal features must be added to the design of privacy-preserving schemes, such as mathematical representations, data structures, unique formulas, and exceptional algorithms. These features introduce another security defense layer or boost the scheme's performance and provide efficient and accountable results. Finally, the designer of privacy-preserving schemes must be ambitious and seek effective and impactful results. The employment of appropriate tools in each design may result in a powerful scheme that can cause the turning tide in the face of security and privacy violations.

CHAPTER 6

A NOVEL MULTI-LAYER ENCRYPTION SYSTEM WITH A ONE-TIME PASSWORD AND MULTI-CLOUD STORAGE STRUCTURE FOR PRIVACY IN CLOUD STORAGE

6.1 Introduction

The need to formulate new solutions for protecting the privacy and security of the cloud computing environment is increasing periodically and quickly. Where security and privacy violations have taken a huge part in weakening the structure of the current technologies and might present a serious threat to individuals, organizations, and governments. Throughout our study, we witnessed the relevance of the privacy-preserving techniques and how it impacts several cloud areas. We also conducted a comparative study between several privacy-preserving approaches to observe the positive and negative issues that can aid in the development of the best possible solution for cloud storage security. The outcomes of chapter 4 and 5 are very encouraging, and it can guide us towards proposing the design of a novel framework in which user and data privacy is protected inside a cloud environment. In this chapter, and based on this study, a privacy-preserving framework is proposed that uses a multi-layer encryption system with the use of one-time password technology. Our vision for this framework is to achieve confidentiality and authentication by using the multi-layer encryption system. Simultaneously, creating another authentication level using one-time password technology can form another defense barrier against identity theft attacks. Nevertheless, the proposal of the new framework will put the base for future researchers in the field of cloud computing security. And it will guide further towards

the design of efficient and reliable approaches that build a secure future for cloud and IT industries.

6.2 Design principles of privacy-preserving techniques

For the past several years, privacy-preserving approaches have been developed with different variations and a distinctive number of security characteristics. But only a limited number of these approaches were compiled to the design principles and followed a specific type of cloud security policies. Where all cloud security countermeasures must satisfy several rules and policies regarding encryption, auditing, implementing access control mechanisms, and splitting data into a multi-cloud storage environment [167], [168]. The design of privacy and security countermeasures is a very sensitive subject because many organizations and internet services like the cloud rely heavily on what to offer by these countermeasures. As a mandatory aspect of cloud security, we will briefly discuss what type of design elements need to be considered before establishing the work with the new privacy-preserving framework. There are several principles that achieve the optimal solution to the problems of a data breach [169]:

1- Proper Knowledge of the technology and its infrastructure: the designer of the security system must have adequate education and understanding of the current technology (Cloud computing). So, it will be easy for him to overcome any design or post-launch problems.

2- Protection for the active data: data transmitting inside the cloud network need protection against different cryptographic attacks. It is recommended to encrypt data with proper encryption techniques at every stage in the cloud network.

3- Inclusion of access control and authentication methods: it is important to adopt the means to control and govern the cloud network's access. Access control mechanisms are the key to a secure and unbreachable network environment.

4- Auditing and inspection techniques: the supervision of the network traffic is something extremely recommended. Auditing approaches create a guard post that keeps system contributors and data traffic under surveillance to discover any suspicious or unusual acts if there are network activities.

5- Data segmentation and distribution: splitting data into smaller portions or segments has proven to be a unique method to hide sensitive data. Also, cloud computing technology has offered the ability to outsource the chunks of data to a multi-cloud storage system.

6- Privacy policies and regulations: a set of rules and standards must be established during the design of the privacy-preserving technique, which governs the control and use of cloud computing services. Network participants must comply with these rules before establishing any connection inside the cloud network.

6.3 The MLES structure and design elements

In the MLES framework design, we relied heavily on the results extracted previously from the seven privacy-preserving approaches in terms of advantages, limitations, and abnormalities. In this section, we will put these unique outcomes into a novel framework that can protect cloud storage from data privacy violations. The following components will describe the structure of the MLES framework, and the design features included within its structure:

1- System participants: for this framework, we presented three parties, including system admin, user, and cloud service provider. The system administrator is responsible for several key activities in the system, such as creating a privileged users list, receive data to perform first encryption (AES), and so on. However, normal users want to interact with the cloud service provider securely. Lastly, the cloud service provider offers several types of services to the users, such as a Multi-storage system, processing, and network.

2- User interface and Registration system: A registration system is imported in order to give regular users the ability to interact and enlist with the system and take full advantage of the system functionalities and cloud services.

3- Data controller function: It is required to add a data handler mechanism so it can be a feasible task to store and retrieve data to/from cloud storage through a cloud service provider.

4- Data processing and pre-encryption function: in our framework, we settled to add a slightly different approach toward plain data processing. We added the ability to split and merge data segments in order to create some diffusion. The implementation of the Advanced Encryption Standard (AES) will give the ability to the clients to encrypt their data before outsourcing to the cloud environment.

5- Auditing approach: It is preferred to use internal auditing, which is performed by system admin/ data owner instead of the third-party auditor because internal auditing offers more secure and restricted inspection over cloud data than a third-party auditor who might have the curiosity to gain sensitive information when possible.

6- Cryptographic techniques: We decided to use two encryption layers and at different levels of the entire system, adding more security restrictions over sensitive data. Our first layer of encryption will be the Advanced Encryption Standard (AES), and it will be implemented by privileged system members While The second layer of encryption will be the Rivest-Shamir-Adleman (RSA), and it will be conducted by the cloud service provider.

7- External assets: one of the unique and new technologies that we would like to adopt for the purpose of authentication is the one-time password. In this framework, the use of the one-time password technique is to create another level of authentication, but this time for system users.

8- Data splitting and data merging algorithms: To increase the level of security in our framework, we decided to adopt data segmentation and data merging algorithms. Data segmentation will split data into smaller segments before the encryption process, while data merging will combine all the resultants segments (from the decryption process) into the final result, which can be assumed as the plaintext or the original data.

9- Multi-cloud storage structure: we recommend this type of cloud storage to store a different number of data segments inside each cloud storage node. The multi-storage structure offers service availability in case of storage failure. Further, the multi-cloud storage structure has another unique feature, which is data anonymization. That is why we wanted this type of storage to achieve both service availability and data anonymization features.

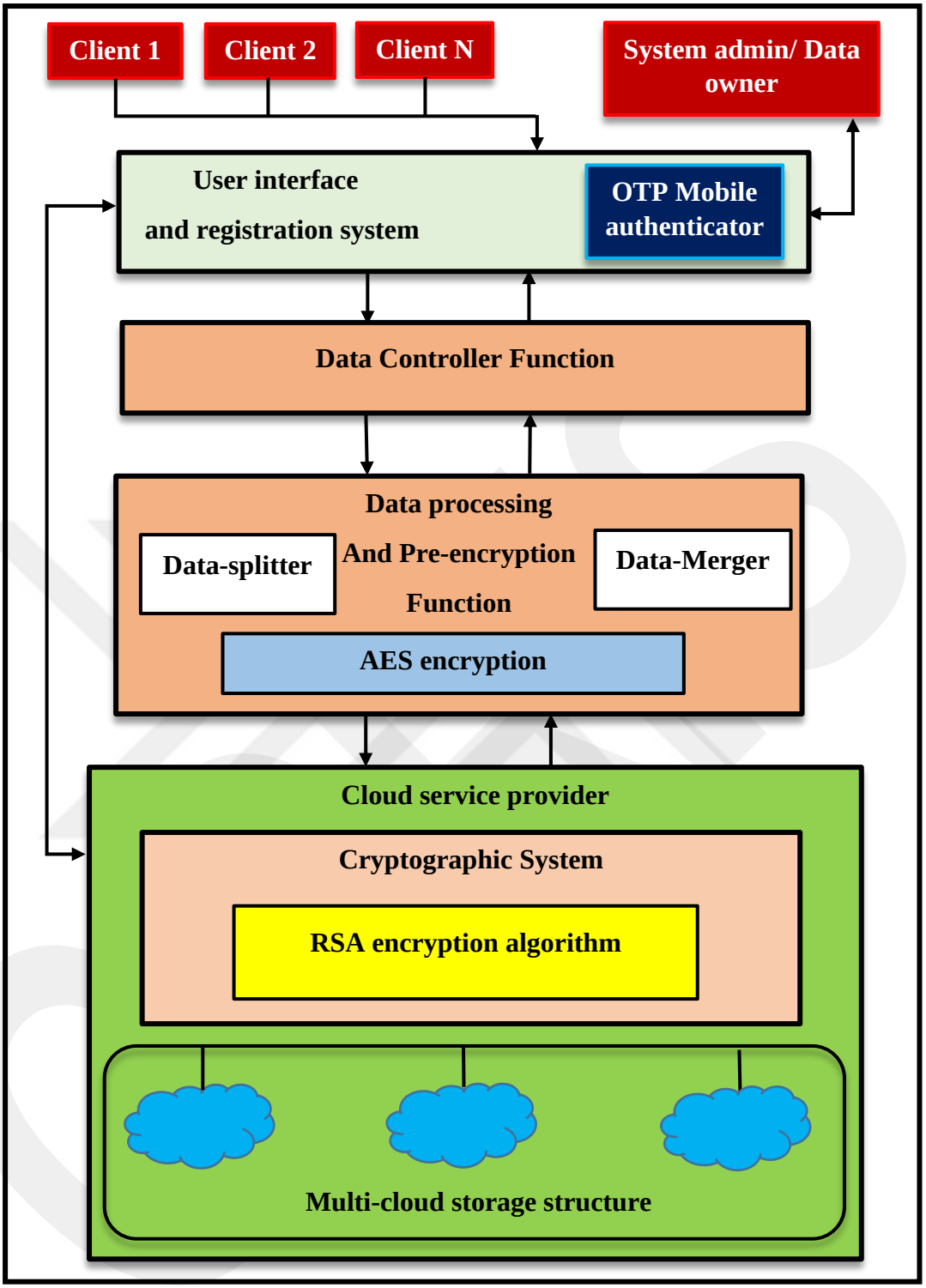

Figure 6.1 Multi-layer encryption system with a one-time password and multi-cloud storage structure

6.3.1 Summary of the MLES figure

As we can obtain from the MLES figure, the multi-layer encryption framework consists of several design functions, including system participants, user interface and registration system, data controller function, data processing and pre-encryption function, and cloud service provider cryptographic system. Each of these functions has its own way to establish, process, encrypt/decrypt, and transfer data. The main contributors in the system are the clients, system administrator/data owner, and cloud service provider. The system administrator is responsible for the auditing and inspection operations such as checking the authenticity of system participants, an inspection of the transmitted data, and risk assessment of possible security and privacy attacks. The user interface presents a suitable environment for the clients to allow them for better interaction with the system and cloud network. The data controller is the intermediate where data is assigned with activities such as store and retrieve operations.

Data processing and pre-encryption function are responsible for pre-processing of the plain data to make it ready for the first layer of encryption. Finally, the cryptographic system is the main function of this framework. The cryptographic system enhances data security by adding a second layer of encryption, making the security characteristics that encapsulate data even stronger.

6.4. The MLES workflow

6.4.1. Registration process

In the beginning, clients can access the functionality of the system by performing a registration process. Each client needs to enter their identification information in the registration form so it can be collected and imported into a list that includes all the privileged users of the system. The clients must enter a mobile phone number and install the one-time password application to become an eligible user in the system to receive the authentication codes. After the registration process is complete

for each independent user, the registration system will create a privileged users' list and sends it to both the system administrator and cloud service provider.

6.4.2. The process of storing data into the cloud storage

Data encryption is a straightforward process; system admin/data owner and members of the privileged user list can store their data in the cloud by performing a multi-layer encryption process over the plain data. Clients can start the process by sending a store request to the system administrator/ data owner. If the system administrator can authenticate the user who sends the store request by referring to the privileged user list, the system administrator sends a second authentication code to the one-time password application and inform the client that he/she needs to enter the authentication code so he/she can be procced with the store operation. After that, clients procced with store operation by handing the plain data to the data controller function, which directs the data towards the data processing and pre-encryption function. As the first stage in the data processing function, the client starts to process the data by splitting it into multiple data segments. Each segment will be encrypted with the same function by applying the AES (Advanced Encryption Standard) as the first encryption layer.

In the next step, the resultant encrypted segments will be directed to the cloud service provider to complete the store operation. However, we wanted to implement another line of defense to the encrypted data, so we have added the Rivest-Shamir-Adleman (RSA) to the cloud service provider. After performing the second layer of encryption over the data segments, all the encrypted data segments will be sent to different clouds based on the use of a multi-cloud storage structure.

6.4.3. The process of retrieving data from the cloud storage

In the beginning, privileged clients send a retrieve operation request to the system admin/ data owner. The same authentication process applies here where the system administrator checks for the client's authenticity by sending a one-time password code to the client's mobile authenticator application. Clients can proceed

with the retrieve operation if they submit the correct authentication code. As the first step of data retrieval, the cloud service provider sends a query to the client who wants to retrieve the data segments from cloud storage. The query will ask the client to submit the private key of the client, so the cloud service provider can decrypt (because the cloud service provider encrypted the data with a public-key shared between the two parties) the outer layer, which is encrypted by (RSA) and send it to the client. Later on, the decrypted form of the segments will reach the data processing function to execute the decryption process over the inner layer and import data segments into the data merging algorithm to extract the original form of the stored data. In the last step, the data processing function will hand the original data form to the data controller, which directs it to the user interface. However, before passing the data to the client, the user interface sends the extracted data to the system administrator for the final review to verify the data integrity.

CHAPTER 7

CONCLUSION

7.1 Introduction

The privacy-preserving technique is an entity's ability to conceal important and critical information to prevent malicious attempts from endangering data contents. Privacy-preserving is crucial, and it is mandatory to implement this concept in a variety of digital environments. However, privacy-preserving schemes are designed to overcome the great dilemma of security and privacy contraventions in different IT sectors. Privacy-preserving schemes are built based on the combination of several elements that form the entire scheme's structure. However, security and privacy perils are lurking around as more advancements in the field of informatics and the cyber world occur. Security and privacy menaces are evolving daily, and cloud computing has proven to be one of the most vulnerable environments against divergence number of threats.

This thesis presents an example of the nature of privacy-preserving techniques, which are the emerging technology in cybersecurity these days. In this thesis, we adopted a comparative study for seven different privacy-preserving schemes, including Sheren et al. scheme for data confidentiality and access control, Yuan et al. scheme for data sharing security in cloud storage, Ganapathy, S et al. scheme for user authentication and access control, T. Subha et al. scheme for integrity checking of transmitted data. Yu Jin et al. scheme for data hiding approach of cloud storage contents, Zhen Yang et al. scheme for user authentication and confidential auditing, and Liu Guoxiu et al. scheme for creating a secure database with privacy preservation capabilities. The comparative study has considered 16 different privacy attributes to use as comparison

parameters to perform a comprehensive and coherent analysis of privacy-preserving schemes. We choose these schemes based on several theories and key factors, including the use of versatile approaches for privacy preservation, the strong relationship between privacy attributes in all sorts of schemes, complexity level, resources consumption, and the exclusive addressing of cloud storage security and privacy attacks. Our comparison results also show some similarities, differences, advantages, and limitations in these schemes based on the use of various privacy attributes. We also proposed a novel multi-layer encryption system to protect cloud storage contents by integrating the one-time password authentication technique and a multi-cloud storage structure. In the proposed framework, we took into consideration the results extracted from the comparison study of different privacy-preserving schemes and the design principles' core steps to create a suitable and reliable cloud security system that can handle any attempt to endanger cloud data contents.

7.2 Limitations

Although there are several advantages to conduct this type of study, however, these kinds of studies are not clear of disadvantages and constraints. Throughout our research and the use of different methodologies to complete such subjects, we found several limitations to our study that are worth mentioning. The main limitation of this study is the use of complex schemes of privacy-preserving for cloud storage. In fact, complicated structures of privacy-preserving schemes contain a significant amount of complex mathematical representations and tangled algorithms that are time-consuming. These schemes require a huge effort to analyze and understand as each scheme requires a special methodology to convert and interpret into a simpler and slightly feasible form that researchers can understand.

7.3 Future works

The study on the subject of privacy preservation is expanding on a daily basis. Because this specific subject type has a significant demand in the last several years

due to the services and functionalities it provides. Such a study can be extended in terms of widening the search area for new privacy-preserving schemes that are simpler and efficient and selecting more reliable and accountable privacy attributes that can strengthen the study's overall outcome. Our vision for the future is to continue the development and improvements in the MLES framework. The aim is to enhance the structure of the framework by adding more cryptographic techniques with respect to the efficiency of the framework. In addition, there are some improvements to several features in the authentication system that need to be considered, such as implementing additional authentication techniques or even creating new and reliable authentication applications. Also, several problems need to be investigated about including risk assessment criteria of possible attacks and new methodologies for pre-processing data. Also, we want to find a suitable method for implementing cloud scalability into our framework, so we can add a level of adaptability to the framework in case the cloud service provider decided to expand his infrastructure. Finally, The results extracted from the comparative study are unique and unmatched compared to any other research about the same subject. These results can set up a guideline for future research in the same field to create a safe, reliable, and efficient cloud computing environment.

REFERENCES

[1] A. Ahmad Dar, “Cloud Computing-Positive Impacts and Challenges in Business Perspective,” *J. Comput. Sci. Syst. Biol.*, vol. 12, no. 01, 2018.

[2] J. Domingo-Ferrer and A. Blanco-Justicia, “Privacy-Preserving Technologies,” in *The International Library of Ethics, Law and Technology*, Cham: Springer International Publishing, 2020, pp. 279–297.

[3] L. Wang *et al.*, “Cloud computing: A perspective study,” *New Gener. Comput.*, vol. 28, no. 2, pp. 137–146, 2010.

[4] Y. Sun, J. Zhang, Y. Xiong, and G. Zhu, “Data Security and Privacy in Cloud Computing,” *International Journal of Distributed Sensor Networks*, vol. 10, no. 7, p. 190903, Jul. 2014.

[5] M. Thangavel, P. Varalakshmi and S. Sridhar, "An analysis of privacy preservation schemes in cloud computing," *in 2016 IEEE International Conference on Engineering and Technology (ICETECH)*, Coimbatore, 2016, pp. 146-151. [Accessed Feb. 21, 2020].

[6] Williams, “Research Methods”, *JBER*, vol. 5, no. 3, Mar. 2007.

[7] S. Trivedi, *Handbook of research on advanced data mining techniques and applications for business intelligence*. IGI Global, 2017, p. 438.

[8] R. Mendes and J. P. Vilela, “Privacy-preserving data mining: Methods, metrics, and applications,” *IEEE Access*, vol. 5, pp. 10562–10582, 2017.

[9] S. JeurNagaraj and P. Kumar, “Review on Privacy-Preserving in Cloud Computing,” *International Journal of Computer Applications*, p. 4, 2014.

[10] ” *Thoughtworks.com*, 30-Jun-2017. [Online]. Available: https://www.thoughtworks.com/insights/blog/building-privacy-preserving-architecture-less-server-trust. [Accessed Feb. 29, 2020].

[11] T. Ercan, “Effective use of cloud computing in educational institutions,” *Procedia Soc. Behav. Sci.*, vol. 2, no. 2, pp. 938–942, 2010.

[12] N. Joseph, E. Daniel, and N. Vasanthi, “Survey on privacy-preserving methods for storage in cloud computing,” *International Journal of Computer Applications*, 2013.

[13] P. S. Dubey, P. A. Dhakulkar, A. A. Gaikwad, and S. P. Dhokane, “Privacy preserving keyword search over cloud data,” *Irjet.net*. [Online]. Available: https://www.irjet.net/archives/V5/i3/IRJET-V5I3281.pdf. [Accessed March. 05, 2020].

[14] S. Bhagyashri and Y. B. Gurav, “A survey on privacy-preserving techniques for secure cloud storage,” *Ijcsmc.com*. [Online]. Available: https://ijcsmc.com/docs/papers/February2014/V3I2201499a24.pdf. [Accessed March. 08, 2020].

[15] Y. Liu, Y. L. Sun, J. Ryoo, S. Rizvi, and A. V. Vasilakos, “A survey of security and privacy challenges in cloud computing: Solutions and future directions,” *J. Comput. Sci. Eng.*, vol. 9, no. 3, pp. 119–133, 2015.

[16] *“Trust in cloud computing”* [Online]. Available: http://ijarcet.org/wp-content/uploads/IJARCET-VOL-2-ISSUE-4-1541-1548.pdf. [Accessed March. 10, 2020].

[17] “Trusted Computing - IEEE Access,” *Ieee.org*, 09-May-2017. [Online]. Available: https://ieeeaccess.ieee.org/special-sections-closed/trusted-computing/. [Accessed: 11- March- 2020].

[18] T.-F. Fortis and V. I. Munteanu, “Steps towards cloud governance. A survey,” in *Proceedings of the ITI 2012 34th International Conference on INFORMATION TECHNOLOGY INTERFACES*, 2012, pp. 29–34.

[19] N. Singh and A. K. Singh, “Data privacy protection mechanisms in cloud,” *Data Sci. Eng.*, vol. 3, no. 1, pp. 24–39, 2018.

[20] L. Gundert, “Understanding security through probability - Cisco blogs,” *Cisco.com*, 20-Mar-2014. [Online]. Available: https://blogs.cisco.com/security/understanding-security-through-probability. [Accessed March. 15, 2020].

[21] G. Cormode and D. Srivastava, “Anonymized data: Generation, models, usage,” in *Proceedings of the 35th SIGMOD international conference on Management of data - SIGMOD ’09*, 2009.

[22] *Iitb.ac.in*.[Online].Available:https://www.cse.iitb.ac.in/archive/internal/techreports/reports/TR-CSE-2010-31.pdf.[Accessed March. 20, 2020].

[23] K. Karthiban and S. Smys, “Privacy preserving approaches in cloud computing,” *in 2018 2nd International Conference on Inventive Systems and Control (ICISC)*, 2018, pp. 462–467.

[24] P. Pavani and D. R. E. Kesavulu Reddy, “A novel efficient remote data possession checking protocol in cloud storage,” *Ijsetr.com*. [Online]. Available: http://ijsetr.com/uploads/432165IJSETR16627-89.pdf. [Accessed March. 26, 2020].

[25] Waqar, A., Raza, A., Abbas, H., & Khan, M. K. (2013). A framework for preservation of cloud users’ data privacy using dynamic reconstruction of metadata. *Journal of Network and Computer Applications*, 36(1), 235-248.

[26] R. Kumar and R. Goyal, “On cloud security requirements, threats, vulnerabilities and countermeasures: A survey,” *Comput. Sci. Rev.*, vol. 33, pp. 1–48, 2019.

[27] *Cloudsecurityalliance.org*.[Online].Available:https://downloads.cloudsecurityalliance.org/assets/research/securityguidance/security-guidance-v4-FINAL.pdf. [Accessed April. 03, 2020].

[28] S. A. El-Booz, G. Attiya and N. El-Fishawy, "A secure cloud storage system combining Time-based One Time Password and Automatic Blocker Protocol," *in 2015 11th International Computer Engineering Conference (ICENCO)*, Cairo, 2015, pp. 188-194.

[29] J. Rydell, M. Pei, and S. Machani, "TOTP: Time-based one-time password algorithm," 2011.

[30] B. Preneel, "Cryptographic hash functions," *Eur. trans. telecommun.*, vol. 5, no. 4, pp. 431–448, 2010.

[31] K. Kiran, K. Padmaj, and P. Radha, "Automatic protocol blocker for privacy-preserving public auditing in cloud computing", *IJCST*, Vol. 3, Issue. 1, Jan – March, pp. 33-36, 2012.

[32] C Wang, Q Wang, K Ren, W Lou, Privacy preserving public auditing for secure cloud storage. *IEEE Transactions on Computers 62(2)*, 362–375 (2011)

[33] C Wang, Q Wang, K Ren, W Lou, Towards secure and dependable storage services in cloud computing. *IEEE Trans. on Services Computing 5(2)*, 220–232 (2012)

[34] T. Fydorenchyk, "Apache Tomcat server cloud hosting with jelastic PaaS," *Jelastic.com*, 05-Jun-2018. [Online]. Available: https://jelastic.com/blog/tomcat-server-cloud-hosting/. [Accessed April. 10, 2020].

[35] "OWASP Top ten web application security risks | OWASP," *Owasp.org*. [Online]. Available: https://owasp.org/www-project-top-ten/. [Accessed April. 12, 2020].

[36] *Owasp.org*. “release” [Online]. Available: https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Testing_Guide_v4.pdf. [Accessed April. 15, 2020].

[37] D. Yuan et al., “An ORAM-based privacy preserving data sharing scheme for cloud storage,” *J. Inf. Secur. Appl.*, vol. 39, pp. 1–9, 2018.

[38] E. KILTZ and G. NEVEN, ruhr-uni-bochum, 2020. [Online]. Available: https://homepage.ruhr-uni-bochum.de/Eike.Kiltz/papers/ibschapter.pdf. [Accessed April. 21, 2020].

[39] L. Xian and W. Tingthanathikul, “Advanced Encryption Standard (AES) in Counter mode,” 2004.

[40] E. Stefanov et al., "Path ORAM: An Extremely Simple Oblivious RAM Protocol", *Eprint.iacr.org*, 2020. [Online]. Available: https://eprint.iacr.org/2013/280.pdf. [Accessed April. 24, 2020].

[41] “The most popular database for modern apps", MongoDB. [Online]. Available: https://www.mongodb.com/. [Accessed April. 25, 2020].

[42] “ibe-0.7.2 The Stanford IBE library is a 联合开发网 - pudn.com", Pudn.com. [Online]. Available: http://www.pudn.com/Download/item/id/331477.html. [Accessed April. 27, 2020].

[43] T. Elgamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” *IEEE Trans. Inf. Theory*, vol. 31, no. 4, pp. 469–472, 1985. [Accessed April. 29, 2020].

[44] S. Bragg and S. Bragg, "Amortized cost — AccountingTools", AccountingTools, 2020. [Online]. Available: https://www.accountingtools.com/articles/what-is-amortized-cost.html. [Accessed May. 02, 2020].

[45] B. Prabhu kavin and S. Ganapathy, "A secured storage and privacy-preserving model using CRT for providing security on cloud and IoT-based applications," *Comput. netw.*, vol. 151, pp. 181–190, 2019.

[46] H. C. A. van Tilborg, "Chinese Remainder Theorem," in *Encyclopedia of Cryptography and Security*, Boston, MA: Springer US, 2011, pp. 201–202.

[47] C. Margaret and J.M. Steven, *Th e Mathematics of Encryption An Elementary Introduction*, [Online], 29, Available: https://www.ams.org/books/mawrld/029/mawrld029-endmatter.pdf. [Accessed May. 03, 2020].

[48] R. Buyya, "The CLOUDS lab: Flagship projects - gridbus and cloudbus," *Cloudbus.org*. [Online]. Available: http://www.cloudbus.org/cloudsim/. [Accessed May. 05, 2020].

[49] S. Singh , A. Sharma , Analysis of EnDeCloudReports for encrypting and decrypt- ing data in cloud, *Int. J. Comput. Appl.*, 136 (12) (2016) 12–16

[50] T. Subha and S. Jayashri, "Efficient privacy preserving integrity checking model for cloud data storage security," in *2016 Eighth International Conference on Advanced Computing (ICoAC)*, 2017

[51] T. Subha and Dr. S. Jayashri, "Data Integrity Verification in hybrid cloud using TTPA," Lecture Notes in Electrical Engineering 284, *Springer*, pp 149- 159

[52] R. C. Merkle, "A Certified Digital Signature," in *Advances in Cryptology — CRYPTO' 89 Proceedings*, New York, NY: Springer New York, 2007, pp. 218–238. [Accessed May. 10, 2020].

[53] "hjp: doc: RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile," *Hjp.at*. [Online]. Available: https://www.hjp.at/doc/rfc/rfc2459.html. [Accessed May. 13, 2020].

[54] Q.Wang, C.Wang, J.Li, K.Ren, and W.Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proc. of ESORICS'09. Saint Malo, France: Springer-Verlag, 2009, pp.355-370

[55] M. S. Niaz and G. Saake, "Merkle hash tree based techniques for data integrity of outsourced data," *E-tarjome.com*. [Online]. Available: https://e-tarjome.com/storage/btn_uploaded/2020-03-10/1583841544_10496-etarjome%20English.pdf. [Accessed May. 14, 2020].

[56] "Eucalyptus," *Eucalyptus.cloud*. [Online]. Available: https://www.eucalyptus.cloud/. [Accessed May. 17, 2020].

[57] Y. Jin and Y. Wang, "An improved scheme of privacy preserving based on Lagrange interpolation in cloud storage," *in Proceedings of the 2016 2nd International Conference on Artificial Intelligence and Industrial Engineering (AIIE 2016)*, 2016

[58] D. A. Quadling, "Lagrange's interpolation formula," *Math. Gaz.*, vol. 50, no. 374, pp. 372–375, 1966.

[59] "Apache Cassandra," *Apache.org*. [Online]. Available: https://cassandra.apache.org/. [Accessed May. 19, 2020].

[60] C. Guindon, "SWT: The standard widget toolkit | the Eclipse Foundation," *Eclipse.org*. [Online]. Available: https://www.eclipse.org/swt/. [Accessed May. 20, 2020].

[61] Y. Jin, Y. Wang, W. Xia, L. Deng, and H. He, "A data hiding scheme based on Lagrange interpolation algorithm and multi-clouds," *in 2015 Seventh International Symposium on Parallel Architectures*, Algorithms and Programming (PAAP), 2015, pp. 210–216.

[62] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[63] M. A. Alzain, B. Soh, and E. Pardede, “MCDB: Using multi-clouds to ensure security in cloud computing,” *in 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing*, 2011, pp. 784–791.

[64] Z. Yang, W. Wang, Y. Huang, and X. Li, “Privacy-preserving public auditing scheme for data confidentiality and accountability in cloud storage,” *Chin. J. Electron.*, vol. 28, no. 1, pp. 179–187, 2019.

[65] R. A. Popa, J. R. Lorch, D. Molnar, H. J. Wang, and L. Zhuang, “Enabling security in cloud storage SLAs with CloudProof,” *in Proceedings of the 2011 USENIX conference on USENIX annual technical conference*, 2011, p. 31..

[66] “Third party auditing – certification of management systems | ISONIKE ltd,” *Isonike.com*. [Online]. Available: https://www.isonike.com/?q=node/76. [Accessed May. 22, 2020].

[67] W. Stallings, *Cryptography and network security: Principles and practice*, 2nd ed. Upper Saddle River, NJ: Pearson, 1998.

[68] M. Luby and J. Staddon, “Combinatorial bounds for broadcast encryption,” in *Lecture Notes in Computer Science*, Berlin, Heidelberg: Springer Berlin Heidelberg, 1998, pp. 512–526.

[69] “QSDB: An encrypted database model for privacy-preserving in cloud computing,” *KSII Trans. Internet Inf. Syst.*, vol. 12, no. 7, 2018.

[70] A. Biryukov, “Ciphertext-Only Attack,” in *Encyclopedia of Cryptography and Security*, Boston, MA: Springer US, 2011, pp. 207–207.

[71] A. Biryukov, “Chosen Plaintext Attack,” in *Encyclopedia of Cryptography and Security*, Boston, MA: Springer US, 2011, pp. 205–206.

[72] Computer Security Division, Information Technology Laboratory, National Institute of Standards, Technology, and U.S. Department of Commerce, "Block Cipher Techniques," *Nist.gov*, 04-Jan-2017. [Online]. Available: https://csrc.nist.gov/projects/block-cipher-techniques. [Accessed May. 25, 2020].

[73] D. Liu, and S. W. †, "Nonlinear order preserving index for encrypted database query in service cloud environments," *Concurrency and Computation Practice and Experience*, Vol. 25, 2013, pp. 1967–1984. Article (CrossRef Link)

[74] M. Ogburn, C. Turner, and P. Dahal, "Homomorphic encryption," *Procedia Comput. Sci.*, vol. 20, pp. 502–509, 2013.

[75] D. Liu and S. Wang, "Query encrypted databases practically," in *Proceedings of the 2012 ACM conference on Computer and communications security - CCS '12*, 2012.

[76] R. A. Popa, C. M. S. Redfield, N. Zeldovich, and H. Balakrishnan, "CryptDB: Protecting confidentiality with encrypted query processing," *in Proc. of ACM Symposium on Operating Systems Principles 2011*, SOSP 2011, Cascais, Portugal, October, pp. 85-100. Article (CrossRef Link)

[77] W. Wang, "Privacy: The characteristics of privacy and reasons of sharing privacy," *Medium*, 21-Nov-2016. [Online]. Available: https://medium.com/@winniewanghuiyun/privacy-the-characteristics-of-privacy-and-reasons-of-sharing-privacy-b89df9775ef.[Accessed May. 18, 2020].

[78] Lu, X., Qu, Z., Li, Q., & Hui, P. (2015). Privacy Information Security Classification for Internet of Things Based on Internet Data. *International Journal of Distributed Sensor Networks*. https://doi.org/10.1155/2015/932941. [Accessed June. 02, 2020].

[79] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," *Inf. Sci. (Ny)*, vol. 305, pp. 357–383, 2015.

[80] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," *IEEE Commun. Surv. Tutor.*, vol. 15, no. 2, pp. 843–859, 2013.

[81] I. Gul, A. ur Rehman, and M. H. Islam, "Cloud computing security auditing," *in The 2nd International Conference on Next Generation Information Technology*, 2011, pp. 143–148.

[82] "Cryptography in the cloud: Securing cloud data with encryption," *Digitalguardian.com*, 08-Jun-2015. [Online]. Available: https://digitalguardian.com/blog/cryptography-cloud-securing-cloud-dataencryption. [Accessed June. 06, 2020].

[83] *"*Cryptographic Key Management Issues & Challenges in Cloud Services "[Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7956.pdf. [Accessed June. 08, 2020].

[84] B. Schneier, "Key Management," in *Applied Cryptography, Second Edition*, Indianapolis, Indiana: John Wiley & Sons, Inc., 2015, pp. 169–187.

[85] J. Domingo-Ferrer and A. Blanco-Justicia, "Privacy-Preserving Technologies," in *The International Library of Ethics, Law and Technology*, Cham: Springer International Publishing, 2020, pp. 279–297.

[86] N. Khanghahi and R. Ravanmehr, "Cloud computing performance evaluation: Issues and challenges," *Int. J. Cloud Comput. Serv. Archit.*, vol. 3, no. 5, pp. 29–41, 2013.

[87] "Addressing Cybersecurity Vulnerabilities," *Isaca.org*. [Online]. Available: https://www.isaca.org/resources/isaca-journal/issues/2015/volume-5/addressing-cybersecurity-vulnerabilities. [Accessed June. 12, 2020]

[88] Get Connected Blog, "The importance of product certification," *Nordicsemi.com*. [Online]. Available: https://blog.nordicsemi.com/getconnected/the-importance-of-product-certification. [Accessed June. 13, 2020]

[89] "What are cloud testing environments?," *Getzephyr.com*. [Online]. Available: https://www.getzephyr.com/insights/what-are-cloud-testing-environments. [Accessed June. 19, 2020]

[90] "Cloud or clouds? How and why to choose single or multi-cloud" *Stratoscale.com*. [Online]. Available: https://www.stratoscale.com/blog/it-leadership/cloud-clouds-choose-single-multi-cloud-approach/. [Accessed June. 22, 2020]

[91] B. Halpert, Auditing cloud computing: A security and privacy guide. Chichester, England: John Wiley & Sons, 2011.

[92] J. Finney, "Cloud audits and compliance: What you need to know," *Linfordco.com*, 05-Feb-2020. [Online]. Available: https://linfordco.com/blog/cloud-computing-audits/. [Accessed June. 27, 2020]

[93] D. Brand, "Internal audit's role in cloud computing," *EDPACS*, vol. 46, no. 2, pp. 1–10, 2012.

[94] S. More and S. Chaudhari, "Third party public auditing scheme for cloud storage," *Procedia Comput. Sci.*, vol. 79, pp. 69–76, 2016.

[95] M. Agrawal and P. Mishra, "A Comparative Survey on Symmetric Key Encryption Techniques," *Int. J. Comput. Sci. Eng*, p. 4, 2012.

[96] I. Nasarul, K. V., and R. Mohamed, K. V., "Analysis of various encryption algorithms in cloud computing. *Int J Comput Sci Mob Comput*, vol. 6, no. 7, pp. 90-97, 2017.

[97] G. K. Kumar, “Role of cryptography & its related techniques in cloud computing security,” *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. V, no. VIII, pp. 1511–1520, 2017

[98] “What is decryption?,” *Computerhope.com*. [Online]. Available: https://www.computerhope.com/jargon/d/decrypti.html. [Accessed July. 05, 2020]

[99] E. Dosal, “What is IT Asset Management (ITAM) & Why is It Important?,” *Compuquip.com*, 09-Apr-2020. .

[100] A. Amiruddin, A. A. P. Ratna, and R. F. Sari,“Construction and Analysis of Key Generation Algorithms Based on Modied Fibonacci and Scrambling Factors for Privacy Preservation,” International Journal of Network Security, vol. 21, no. 2, pp. 250–258, Mar. 2019.

[101] Z. K. Abdalrdha, I. H. AL-Qinani, and F. N. Abbas, “Subject review : Key generation in different cryptography algorithm,” *Int. J. Sci. Res. Sci. Eng. Technol.*, pp. 230–240, 2019.

[102] A. K. Lenstra and E. R. Verheul, “Selecting cryptographic key sizes: Extended abstract,” in Public Key Cryptography, Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, pp. 446–465.

[103] R. Stubbs, “Classification of Cryptographic Keys,” *Cryptomathic.com*. [Online]. Available: https://www.cryptomathic.com/news-events/blog/classification-of-cryptographic-keys-functions-and-properties. [Accessed July. 17, 2020].

[104] D. M. Turner (guest), “What is Key Management? a CISO Perspective,” Cryptomathic.com. [Online]. Available: https://www.cryptomathic.com/news-events/blog/what-is-key-management-a-ciso-perspective. [Accessed July. 22, 2020].

[105] Sheikh, “Should you use a key management service with multicloud environments?,” *Equinix.com*, 02-May-2018. [Online]. Available:

https://blog.equinix.com/blog/2018/05/02/should-you-use-a-key management-service-with-multicloud-environments/. [Accessed July. 23, 2020].

[106] Www.f5.com. [Online]. Available: https://www.f5.com/pdf/solution-profiles/hardware-security-module-sp.pdf. [Accessed July. 25, 2020].

[107] "Cryptographic key types", En.wikipedia.org, 2020. [Online]. Available: https://en.wikipedia.org/wiki/Cryptographic_key_types. [Accessed July. 28, 2020].

[108] F. Hu et al., "A review on cloud computing: Design challenges in architecture and security," *J. Comput. Inf. Technol.*, vol. 19, no. 1, p. 25, 2011.

[109] "Cyber security design principles," Gov.uk. [Online]. Available: https://www.ncsc.gov.uk/collection/cyber-security-design-principles/cyber-security-design-principles. [Accessed July. 30, 2020].

[110] *IMO MSC.1/Circ.1212, Guidelines on alternative design and arrangements for SOLAS chapters II-1 and III, 15 December 2006, International Maritime Organization. Regulatory Guidance*

[111] B. Öztayşi and A. C. Kutlu, "Determining the importance of performance measurement criteria based on total quality management using fuzzy analytical network process," in *Advances in Intelligent and Soft Computing*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 391–400.

[112] "Cryptographic attacks: Types of attacks with examples, and how to defend against them | CommonLounge," *Commonlounge.com*. [Online]. Available: https://www.commonlounge.com/discussion/4c8ace459d1840408e487a673cca255d. [Accessed Aug. 03, 2020].

[113] J. Su, "Why cloud computing cyber security risks are on the rise: Report," *Forbes Magazine*, 25-Jul-2019.

[114] C. Avey, J. Matt, A. Reyes, S. Arora, E. Singer, and S. Hooda, "7 key cybersecurity threats to cloud computing - cloud academy," *Cloudacademy.com*, 10-Sep-2019

[115] "Test Environment for Software Testing," *Guru99.com*. [Online]. Available: https://www.guru99.com/test-environment-software-testing.html. [Accessed Aug. 07, 2020].

[116] N. Young, "Cyber security for automatic test equipment," in *2017 IEEE AUTOTESTCON*, 2017.

[117] M. Fritze and K. Schiller-Wurster, "Time to get serious about hardware cybersecurity," *Defenseone.com*, 16-Jan-2018. [Online]. Available: https://www.defenseone.com/ideas/2018/01/time-get-serious-about-hardware-cybersecurity/145210/. [Accessed Aug. 10, 2020].

[118] B. Potter and G. McGraw, "Software security testing," *IEEE Secur. Priv.*, vol. 2, no. 5, pp. 81–85, 2004.

[119] "Why multi-cloud strategy beats single cloud almost every time," *Connectria.com*, 12-Sep-2019. [Online]. Available: https://www.connectria.com/blog/why-multi-cloud-strategy-beats-single-cloud-almost-every-time/. [Accessed Aug. 12, 2020].

[120] TechTarget Contributors, "multi-cloud strategy," *Techtarget.com*, 03-Jan-2020. [Online]. Available: https://searchcloudcomputing.techtarget.com/definition/multi-cloud-strategy. [Accessed Aug. 13, 2020].

[121] "The advantages and disadvantages of multi cloud computing," *Eukhost.com*, 24-Sep-2018. [Online]. Available: https://www.eukhost.com/blog/webhosting/the-advantages-and-disadvantages-of-multi-cloud-computing/. [Accessed Aug. 16, 2020].

[122] B. Dong et al., "Efficient discovery of abnormal event sequences in enterprise security systems," *in Proceedings of the 2017 ACM on Conference on Information and Knowledge Management*, 2017.

[123] "Landing page design principles - anomaly [video]," *Thelandingpagecourse.com*. [Online]. Available: https://thelandingpagecourse.com/landing-page-design-principles-anomaly/. [Accessed Aug. 19, 2020].

[124] K. Johnson, "Information Security highlights 2016-2017 accomplishments," *Unc.edu*, 01-Sep-2017. [Online]. Available: https://its.unc.edu/2017/09/information-security-highlights/. [Accessed Aug. 24, 2020].

[125] E. J. Savitz, "Microsoft sees huge spike in cloud services demand, driving stock higher," *Barrons*, 30-Mar-2020. [Online]. Available: https://www.barrons.com/articles/microsoft-sees-huge-spike-in-cloud-services-demand-driving-stock-higher-51585581927. [Accessed Aug. 25, 2020].

[126] S. Pandey and M. Farik, "Cloud computing security: Latest issues & countermeasures," *Ijstr.org*. [Online]. Available: http://www.ijstr.org/final-print/nov2015/Cloud-Computing-Security-Latest-Issues-Countermeasures.pdf. [Accessed Aug. 30, 2020].

[127] M. Birje, P. Challagidad, M. Tapale, and R. H. Goudar, "Security Issues and Countermeasures in Cloud Computing," 2015.

[128] Y. Haider and S. N., "Confidentiality Issues in Cloud Computing and Countermeasures: A Survey," *in National Conference On Emerging Computer Paradigms 2016At: NMAMIT, Nitte*, 2016, p. 5.

[129] U. Greveler, B. Justus, and D. Loehr, "A privacy preserving system for cloud computing," in *2011 IEEE 11th International Conference on Computer and Information Technology*, 2011.

[130] Y. Yu *et al.*, “Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage,” *IEEE trans. inf. forensics secur.*, vol. 12, no. 4, pp. 767–778, 2017.

[131] Y.-C. Chang and M. Mitzenmacher, “Privacy preserving keyword searches on remote encrypted data,” in *Applied Cryptography and Network Security*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 442–455.

[132] S. G. Worku, C. Xu, J. Zhao, and X. He, “Secure and efficient privacy-preserving public auditing scheme for cloud storage,” *Comput. Electr. Eng.*, vol. 40, no. 5, pp. 1703–1713, 2014.

[133] 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.

[134] Z. Fan, “Research on access control in cloud storage system: From single to multi-clouds,” *Am. j. softw. eng. appl.*, vol. 7, no. 1, p. 1, 2018.

[135] M. Ali et al., "SeDaSC: Secure Data Sharing in Clouds," in IEEE Systems Journal, vol. 11, no. 2, pp. 395-404, June 2017.

[136] G. Bourgeois, “Why cloud storage security is important,” *Hubstor.net*, 02-Mar-2015. [Online]. Available: https://www.hubstor.net/blog/cloud-storage-security-important/. [Accessed Sep. 04, 2020].

[137] S. Kamara and K. Lauter, “Cryptographic Cloud Storage,” in *Financial Cryptography and Data Security*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 136–149.

[138] M. Rady, T. Abdelkader, and R. Ismail, “Integrity and confidentiality in cloud outsourced data,” *Ain Shams Eng. J.*, vol. 10, no. 2, pp. 275–285, 2019.

[139] Y. X. Yan, L. Wu, W. Y. Xu, H. Wang, and Z. M. Liu, “Integrity audit of shared cloud data with identity tracking,” *Secur. Commun. Netw.*, vol. 2019, pp. 1–11, 2019.

[140] W. Akeel and A. Hashim, “Using Steganography for Secure Data Storage in Cloud Computing,” 2017.

[141] X. Liao and C. Shu, “Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels,” *J. Vis. Commun. Image Represent.*, vol. 28, pp. 21–27, 2015.

[142] J. Wu, Y. Li, T. Wang and Y. Ding, "CPDA: A Confidentiality-Preserving Deduplication Cloud Storage With Public Cloud Auditing," in *IEEE Access*, vol. 7, pp. 160482-160497, 2019, doi: 10.1109/ACCESS.2019.2950750.

[143] I. Sakih, “Database security in the cloud,” KTH Royal Institute of Technology, Sweden, 2012.

[144] A. İnan and E. Var, “Sınıflandırma için diferansiyel mahremiyete dayalı öznitelik seçimi,” *Gazi Üniv. Mühendis.-Mimar. Fak. Derg.*, vol. 33, no. 1, 2018.

[145] Y. Nurhajati, “The impact of cloud computing technology on the audit process and the audit profession,” *Ijstr.org*. [Online]. Available: https://www.ijstr.org/final-print/aug2016/The-Impact-Of-Cloud-Computing-Technology-On-The-Audit-Process-And-The-Audit-Profession.pdf. [Accessed Sep. 11, 2020].

[146] F. Doelitzscher, C. Reich, M. Knahl, and N. Clarke, “Understanding Cloud Audits,” in *Computer Communications and Networks*, London: Springer London, 2013, pp. 125–163.

[147] L. Zhang, H. Xiong, Q. Huang, J. Li, K.-K. R. Choo, and J. Li, “Cryptographic solutions for cloud storage: Challenges and research opportunities,” *IEEE trans. serv. comput.*, pp. 1–1, 2020.

[148] "The importance of true randomness in cryptography," *Design-reuse.com*. [Online]. Available: https://www.design-reuse.com/articles/27050/true-randomness-in-cryptography.html. [Accessed Sep. 15, 2020].

[149] H. Tianfield, "Security issues in cloud computing," in *2012 IEEE International Conference on Systems*, Man, and Cybernetics (SMC), 2012, pp. 1082–1089.

[150] M. N. R and S. V. Sathyanarayana, "Key management infrastructure in cloud computing environment-a survey," *ACCENTS trans. inf. secur.*, vol. 2, no. 7, pp. 52–61, 2017.

[151] "The role of the key in Cryptography & cryptosystems | study.Com," *Study.com*. [Online]. Available: https://study.com/academy/lesson/the-role-of-the-key-in-cryptography-cryptosystems.html. [Accessed Sep. 23, 2020].

[152] V. Casola, A. De Benedictis, M. Rak, and E. Rios, "Security-by-design in clouds: A security-SLA driven methodology to build secure cloud applications," *Procedia Comput. Sci.*, vol. 97, pp. 53–62, 2016.

[153] S. J. Knapskog, "Security Evaluation Criteria," *IFAC proc. vol.*, vol. 24, no. 13, pp. 131–134, 1991.

[154] F. Shaikh and S. Haider, "Security threats in cloud computing," in *2011 International Conference for Internet Technology and Secured Transactions, ICITST 2011*, 2011, pp. 214–219.

[155] Y.-H. Tung, C.-C. Lin, and H.-L. Shan, "Test as a service: A framework for web security TaaS service in cloud environment," in *2014 IEEE 8th International Symposium on Service Oriented System Engineering*, 2014, pp. 212–217.

[156] "Cloud Scalability," *Vmware.com*. [Online]. Available: https://www.vmware.com/topics/glossary/content/cloud-scalability. [Accessed Sep. 26, 2020].

[157] R. S. M. L. Patibandla, S. S. Kurra, and N. B. Mundukur, "A study on scalability of services and privacy issues in cloud computing," in *Distributed Computing and Internet Technology*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 212–230.\

[158] Kazemi, Uranus & Boostani, Reza. "Analysis of Scalability and Risks in Cloud Computing," *International Journal of Academic Research in Computer Engineering*, vol. 2, no. 2538–2411, pp. 24–33, Sep. 2017.

[159] A. Tilley, "One business winner amid Coronavirus lockdowns: The cloud," *Wall Street journal (Eastern ed.)*, wsj.com, 27-Mar-2020.

[160] X. Zhang, C. Liu, S. Nepal, W. Dou, and J. Chen, "Privacy-preserving layer over MapReduce on cloud," in *2012 Second International Conference on Cloud and Green Computing*, 2012.

[161] Z. Wan, J. Liu, and R. H. Deng, "HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing," *IEEE trans. inf. forensics secur.*, vol. 7, no. 2, pp. 743–754, 2012

[162] R. Ahuja, S. K. Mohanty, and K. Sakurai, "A scalable attribute-set-based access control with both sharing and full-fledged delegation of access privileges in cloud computing," *Comput. Electr. Eng.*, vol. 57, pp. 241–256, 2017.

[163] X. Zhang, C. Liu, S. Nepal, C. Yang, W. Dou, and J. Chen, "SaC-FRAPP: a scalable and cost-effective framework for privacy preservation over big data on cloud: SAC-FRAPP: A SCALABLE AND COST-EFFECTIVE FRAMEWORK FOR PRIVACY PRESERVATION," *Concurr. Comput.*, vol. 25, no. 18, pp. 2561–2576, 2013.

[164] X. Zhang, C. Yang, S. Nepal, C. Liu, W. Dou, and J. Chen, "A MapReduce based approach of scalable multidimensional anonymization for big data privacy preservation on cloud," in *2013 International Conference on Cloud and Green Computing*, 2013.

[165] J. Dean and S. Ghemawat, "MapReduce: Simplied Data Processing on Large Clusters," *Googleusercontent.com*. [Online]. Available: http://static.googleusercontent.com/media/research.google.com/es/us/archive/mapreduce-osdi04.pdf. [Accessed Sep. 29, 2020].

[166] X. Zhang, L. T. Yang, C. Liu, and J. Chen, "A scalable two-phase top-down specialization approach for data anonymization using MapReduce on cloud," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 363–373, 2014.

[167] Nexor, "Explaining the 14 cloud security principles," *Nexor.com*, 21-Sep-2018. [Online]. Available: https://www.nexor.com/cloud-security-principles/. [Accessed Oct. 05, 2020].

[168] Nutanix, "Cloud security design principles to follow in 2018 - nutanix - medium," *Medium*, 04-Jan-2018. [Online]. Available: https://medium.com/@nutanix/cloud-security-design-principles-to-follow-in-2018-9423d5fa7769. [Accessed Oct. 06, 2020].

[169] "Security on the cloud - design principles - cloud architecture: A guide to design & architect your cloud," *Educative.io*. [Online]. Available: https://www.educative.io/courses/cloud-architecture-a-guide-to-design-and-architect-your-cloud/7nnxwPxALZj. [Accessed Oct. 10, 2020].