fffffffff

by Mohamed Ahmed

Submission date: 17-Oct-2022 12:22AM (UTC+0800)
Submission ID: 1926609361
File name: Mohammed_Ahmed_Salman_AL-KHAFAJI.docx (1.82M)
Word count: 14328
Character count: 76659

REPUBLIC OF TURKEY

ALTINBAS UNIVERSITY

Institute of Graduate Studies

Information Technologies

AN EFFECTIVE AND SECURE PUBLIC DATA INTEGRITY VERIFICATION SCHEME OF CLOUD STORAGE BASED ON BLS SIGNATURE

Mohammed Ahmed Salman AL-KHAFAJI

Master's Thesis

Supervisor

Asst. Prof. Dr. Oguz ATA

Istanbul, 2022

AN EFFECTIVE AND SECURE PUBLIC DATA INTEGRITY VERIFICATION SCHEME OF CLOUD STORAGE BASED ON BLS SIGNATURE

Mohammed Ahmed Salman AL-KHAFAJI

Information Technologies

Master's Thesis

ALTINBAŞ UNIVERSITY

2022

The thesis titled AN EFFECTIVE AND SECURE PUBLIC DATA INTEGRITY VERIFICATION SCHEME OF CLOUD STORAGE BASED ON BLS SIGNATURE prepared by MOHAMMED AHMED SALMAN and submitted on 12/8/2022 has been **accepted unanimously** for the degree of Master of Science in Information Technologies.

_____

Asst. Prof. Dr. Oguz ATA

Supervisor

Thesis Defense Committee Members:

Asst. Prof. Dr. Oguz ATA	Faculty of Engineering and Architecture, Altinbas University	_____
Asst. Prof. Dr. Dogu Cagdas ATILLA	Faculty of Engineering and Architecture, Altinbas University	_____
Asst. Prof. Dr. Aytuğ BOYACI	Air Force Academy, National Defense University	_____

I hereby declare that this thesis meets all format and submission requirements of a master's thesis.

Submission date of the thesis to Institute of Graduate Studies: ___/___/__

I hereby declare that all information/data presented in this graduation project has been obtained in full accordance with academic rules and ethical conduct. I also declare all unoriginal materials and conclusions have been cited in the text and all references mentioned in the Reference List have been cited in the text, and vice versa as required by the abovementioned rules and conduct.

Mohammed Ahmed Salman

Signature

DEDICATION

First and foremost, I dedicate this work to my supervisor, who has been the light that has illuminated my path along the road. My mother, father, brothers, wife, sisters, children, and all of my friends who stood by me in every manner to offer support and whose help was the catalyst that kept me going during all of my difficult moments.

PREFACE

My joy is indescribable, and I am overjoyed that I have progressed to this stage in my master's studies, thanks to my supervisor, Dr Oguz ATA, to whom I am eternally grateful for his guidance and constant assistance, as he assisted in the constant progress and resolution of all problems. In addition to his correct and sound insights, which caused me to take a completer and more impartial look at the study topic. I wouldn't have made it here if it hadn't been for him giving me his time. I am thankful to him for allowing me to collaborate with him on this topic issue.

ABSTRACT

AN EFFECTIVE AND SECURE PUBLIC DATA INTEGRITY VERIFICATION SCHEME OF CLOUD STORAGE BASED ON BLS SIGNATURE

ALKHAFAJI, Mohammed

M.Sc./ Information Technologies, Altınbaş University

Supervisor: Asst. prof. Dr. Oguz ATA

Date: 08 / 2022

Pages: 64

Cloud computing is a concept that allows customers to use cloud-based remote data storage services. With all the advantages of cloud computing, users can no longer have direct access to external data, which makes the process of ensuring the confidentiality of data stored in the cloud even more important. As a result, users may use cloud storage instead of local storage, and they won't have to worry about checking the integrity of their cloud data. As a result, the concepts of confidentiality and data integrity have evolved into two problems that have direct implications for the security and performance efficiency of the cloud system. This is because one of the assumptions of threat models is that cloud providers cannot be completely trusted. In this thesis we focus on solving data security problems, which focuses on two goals, the first is to maintain the confidentiality of data, so the data must be stored in an encrypted file form, and the second aspect relates to the concerns of obtaining data. Therefore, it is necessary to protect the users of cloud computing with an effective method of remote data auditing where the data can be abandoned in the local storage, and this achieves the main objectives of overcoming the challenges in terms of general control, effective performance and high level of security. Because public auditing is one of the most important aspects, this makes TPA audit and data integrity validation a complete reliance of cloud users in the audit process, even though the audit process should not contain any security vulnerabilities towards the data privacy of cloud users nor They bear no burden on the Internet. Therefore, to increase the reliability of TPA verification, there must be a way to preserve user data and privacy while in the cloud. Therefore, in this thesis we propose a secure and efficient system based on the Boneh-Lynn-Shacham (BLS) signature to

ensure the provision of public data audits that are both secure and efficient while maintaining data privacy. And to increase the complexity in terms of security and privacy, we have reformulated the signature equation in addition to the public key equation while maintaining a high speed of system implementation. The system is considered very safe and effective by analyzing the overall performance of the system, as the system is considered to be more efficient, secure and faster compared to the previous works. A dataset (Berka) was used in the proposed system, which is financial information for a Czech bank. As a result, the data audit rate is 100% and does not contain any costs in terms of accounting and communication overheads.

Keywords: Cloud Computing, Public Auditing, Privacy-Preserving, Third-Party-Auditor

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

ABBREVIATIONS

IT : Information Technology

CSP : Cloud Service Provide

BLS : Boneh-Lynn-Shacham

AES: Advanced Encryption Standard

TPA: Third- party auditor

NIST: National Institute of Standards and Technology

SLAs: Service-Level Agreements

RSA: Ron Rivest, Adi Shamir, and Leonard Adleman Algorithm

DES: Data Encryption Standard Algorithm

TEA: Tiny Encryption Algorithm

CDH problem: Computational Diffie-Hellman Problem

SHA256: Secure Hash Algorithm

1. INTRODUCTION

In the Information Technology (IT) organizations the paradigm of cloud computing is the next step because it provides many IT services, such as demand self-service, access to the network from anywhere, fast resource adaptability, location independence, payment based on usage and risk management [1][2]. Cloud computing is a positive experience with significant consequences for how businesses employ technology. One of the most important features of this paradigm is that the data is geared toward cloud computing. One of the important advantages of cloud storage services is that it provides access to data completely and from anywhere around the world and reduces the high costs of purchasing hardware and software, in addition to reducing the overload on data storage management [3]. One of the fundamental technologies in the cloud paradigm is cloud storage. Many systems have addressed cloud storage because of its low cost and great efficiency; as a result, Data centers will be transformed into large-scale computing services as a result of cloud data storage. Customers will be able to experience high-quality cloud services thanks to the rapid development of network bandwidth, as well as network trust and flexibility [4]. Traditional storage systems are not the same as cloud storage. It provides customers with a lot of storage space and allows them to access data from different parts of the world. In other words, from any device that is connected to the network the cloud users can access the data anytime anywhere [5].

This chapter begins with an overview of cloud computing, then moves on to a problem description, aims, and the significance of the thesis, before concluding with a thesis outline.

1.1 MOTIVATION

Despite the numerous advantages of the cloud model, customers who use outsourced data face a number of security concerns. Users will cede control over their data because the CSP's management entities are independent. As a result, Outages, security breaches in cloud computing firms, and threats to cloud computing infrastructures all put user data at risk [4][6]. Furthermore, cloud service providers have numerous incentives to deceive cloud computing users about the status of their external data. Cloud service providers may, for example, recover

storage related to financial issues by discarding unused or occasionally used data, or even actively concealing data accidents, in order to protect their reputation. [7][8]. In short, despite the cloud's cost-effectiveness in storing data on a vast scale and for a long time, there is no guarantee of data integrity. If not addressed properly, this issue may hamper the successful implementation of cloud architecture. Because cloud computing users do not control their data storage, they may not be able to use traditional encryption methods to secure their data [8]. It is not possible to give a suitable solution to download and validate all data due to the high cost of input and output over the network. Furthermore, just identifying data damage when it is accessed is typically insufficient, Users are unable to confirm the authenticity of data that has not been read, and data corruption or loss may be detected too late.

Data verification in the cloud may be costly for cloud users when contrasted to the vast amount of data that can be acquired from external sources and the user's limited resource capability [9][10].

Cloud users should activate the public auditing service for data stored in the cloud computing paradigm to ensure data integrity, allowing them to allow a third party to review external data as needed. Because cloud users are unfamiliar with auditing cloud data integrity, TPA must be used on their behalf to perform this task; it is a quick and straightforward way for users to confirm that data saved in the cloud is correct [11]. In addition to benefiting cloud consumers, the TPA initiative will benefit cloud service providers in terms of modernizing the cloud services platform [7] [12]. As a result, providing public auditing services will be important to establishing this new method correctly, as customers will need a way to analyze risks and acquire trust in the cloud.

Several techniques have recently been described to evaluate data integrity in a cloud computing scenario without retrieving all of the data [4][13][14][15][16]. For integrity checks that are limited to enquiries, some of these systems depend on random sampling, while others rely on integrity checks that cannot be confirmed by the public. Furthermore, some of the approaches discussed above are inappropriate for third-party auditing, while others lack the capacity to do dynamic data modifications. Even if it is insecure and is ineffectual, the systems described

include guaranteeing that privacy is preserved [8][17][18][19]. presents a universal audit system in a cloud model environment that incorporates privacy; however, it is not secure [18]. The vulnerability of this method is due to incorrect identification and the use of private and public characteristics during the signature generating operation. As a result, users' skepticism of the cloud, as well as the concerns outlined in the systems above, prompted us to propose this thesis.

1.2 PROBLEM STATEMENT

Many issues arise when data is stored in the cloud, primarily owing to a loss of physical control. These concerns have a significant impact on data security and cloud computing system performance. As a result, data on the cloud is exposed to a variety of threats. The major security challenges in the cloud environment, such as data confidentiality and data integrity, are the emphasis of this thesis.

a. Data Confidentiality Problem: The data confidentiality issue is becoming more prevalent as data is transferred between Cloud Service Providers (CSP) and users. Because cloud users outsource their data to controlled and somewhat unreliable servers, this is the case.
b. Data Integrity Problem: Involuntary security breaches may occur because users lose physical control over their data when using cloud computing. For example, due to hardware failure, unintentional faults, or outside interference, the CSP may lose users' data. Or that CSP is attempting to conceal the occurrence in order to protect its reputation. In addition, dishonest CSPs will unintentionally reduce redundancy, resulting in serious data errors in terms of recovery or data loss.

1.3 CONTRIBUTION

This thesis offers a system for storing dynamic cloud data in a standard security architecture based on BLS signature to meet the above issues and fill gaps in earlier work. The following are the thesis' main contributions:

a. Proposing a remote data integrity audit system based on BLS that ensures public auditing and privacy preservation, as this study reformulated the public key equation in addition to

the signature equation to increase complexity while maintaining a high speed of execution. Moreover, the proposed system supports the dynamic data process in terms of modification, deletion, and addition.

b. Using the AES encryption method and splitting algorithm, the suggested system ensures data secrecy in cloud storage environments.
c. Performance study and comparisons with similar systems have further confirmed the system's efficiency. The communication overhead of the proposed system is O. (n).

In a cloud computing context, the goal of this thesis is to create a secure and effective data auditing system. Data confidentiality and data integrity are significant elements that must be considered when creating a data protection system in cloud environments, according to security and performance studies. The suggested system's results show that user data confidentiality is protected with improved privacy and security at lower computational costs. Furthermore, with fewer communication costs, data auditing and privacy are maintained efficiently and securely.

1.4 AIM AND OBJECTIVE

The following basic objectives must be taken when starting to build the system:

a. Public auditing: TPA enables cloud data validation on-demand, without the need for full data recovery or additional online costs for cloud customers.
b. Data confidentiality: To be able to ensure the proposed system's security.
c. Data integrity protection: To ensure the security of the proposed system and protect data integrity.
d. Privacy-preserving: To ensure data privacy and content leakage during TPA audit.
e. Data dynamic support: Provides accurate data storage, even when users modify, delete, or add to the cloud.

2. LITERATURE REVIEW

2.1 INTRODUCTION

This chapter aims to give a comprehensive review of cloud computing, including its advantages and disadvantages. In addition to discussing cloud storage difficulties and cloud computing security challenges, the proposed system includes a full description of the technologies employed. Furthermore, the goal of this chapter is to give an analysis of data security-related works based on data integrity's basic qualities. Provide a summary of this chapter at the end.

2.2 CLOUD COMPUTING OVERVIEW

The cloud computing model is one of the most important modern fields, and it is the spirit of technology for the next generation and the organization because it provides many services that are unparalleled in the world of modern technology, such as access to data at any time and from anywhere, and rapid adaptation to resources. You can also pay and manage risk based on usage .Cloud computing provides great and excellent services to customers as it provides a central data service, which is the most important main advantage of this service, Where the old obstacles such as the burden of managing large storage, the possibility of accessing data from various locations, and the high costs of maintaining devices, are nothing but small problems that these services took care of instead of the user[20].

2.2.1 Cloud computing characteristics

Cloud computing is getting increasingly prevalent. Continuous corporate growth needs high processing power and huge data storage systems. Cloud computing enables businesses to grow and securely transfer data from physical sites to the 'cloud,' which can be accessed from anywhere. Cloud Computing has a number of traits that make it one of the fastest-growing businesses today. Cloud services' versatility, in the form of an ever-expanding collection of tools and methodologies, has expedited their adoption across sectors. This article will take you through the most important aspects of cloud computing.[21]:

a. Self-Service on-Demand: The client has computational capabilities such as server time and network storage, and his needs are met automatically, eliminating the need for human interaction with each service provider.

b. Broad Network Access: Network capabilities may be accessed via conventional procedures that make client platforms more useful (such as laptops and mobile phones).

c. Elastic Resource Pooling: Through the use of a multi-tenant model, the service provider's cloud computing resources are pooled in order to provide service to a large number of customers, as well as allocating various physical and virtual resources and dynamically reallocating them in response to consumer demand. Storage, memory, computation, and network bandwidth are examples of these resources.

d. Rapid Flexibility: In order to extend and edit swiftly, capabilities may be offered quickly, flexibly, and in some circumstances automatically. The capabilities are frequently limitless to the user and may be acquired in any number and at any time.

e. Measured Service: Cloud systems may automatically regulate and improve resource usage by applying metering at a specified level of abstraction suited for the kind of service (e.g., storage, bandwidth, processing, and active user accounts). By monitoring, managing, and reporting resource consumption, it gives transparency to both the service provider and the service customer.

2.2.2 Deployment Models

To allow quick loading, most cloud hubs feature tens of thousands of servers and storage devices. It's common to be able to select a geographic location to bring info "closer" to consumers. As a result, cloud computing deployment methods are classified according to their geographical location. Let's look at the many sorts of models to see which one would be ideal for your company's needs.

a. Public Cloud: The title needs no explanation. Public cloud deployment options are suitable for businesses with volatile and rising demands. It's also a great alternative for organizations that have fewer security concerns. As a result, you pay the cloud service provider for

networking, virtualization processing, and available storage over the public internet. This is also an effective delivery method for development and testing teams. Its quick and easy configuration and deployment makes it a good choice for test environments.

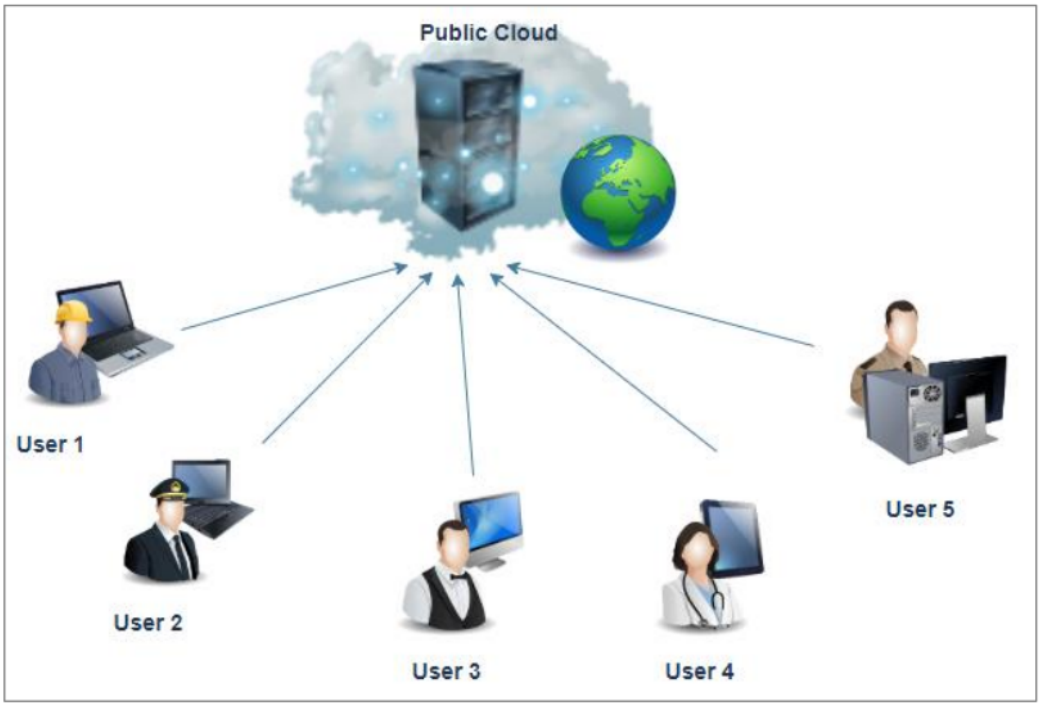

Figure 2.1: Public cloud [21]

b. Private Cloud: Of course, now that you know what the public cloud can do for you, you're curious about what a private cloud can accomplish for you. Companies seeking cost savings and greater control over data and resources will find the private cloud to be a better fit. That is, it will be linked with your data center and controlled by your IT staff. You can also opt to host it somewhere else. When it comes to customization, the private cloud provides more options that can assist fulfill the needs of unique companies. It's also a good solution for mission-critical procedures with constantly changing needs.

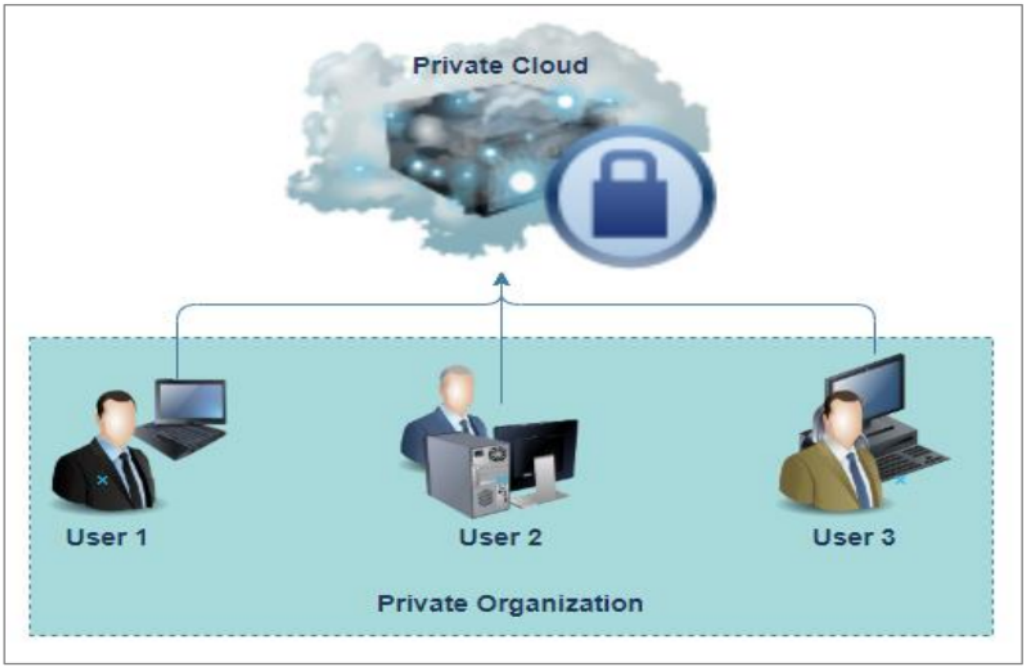

Figure 2.2: Private cloud [21]

c. Community Cloud: The community cloud is comparable to the public cloud in terms of functionality. There's only one difference: it only allows a small number of others with identical interests and uses cases to gain access. Internally or through a third-party supplier, this cloud computing deployment approach is managed and hosted. You may, however, combine all three options.

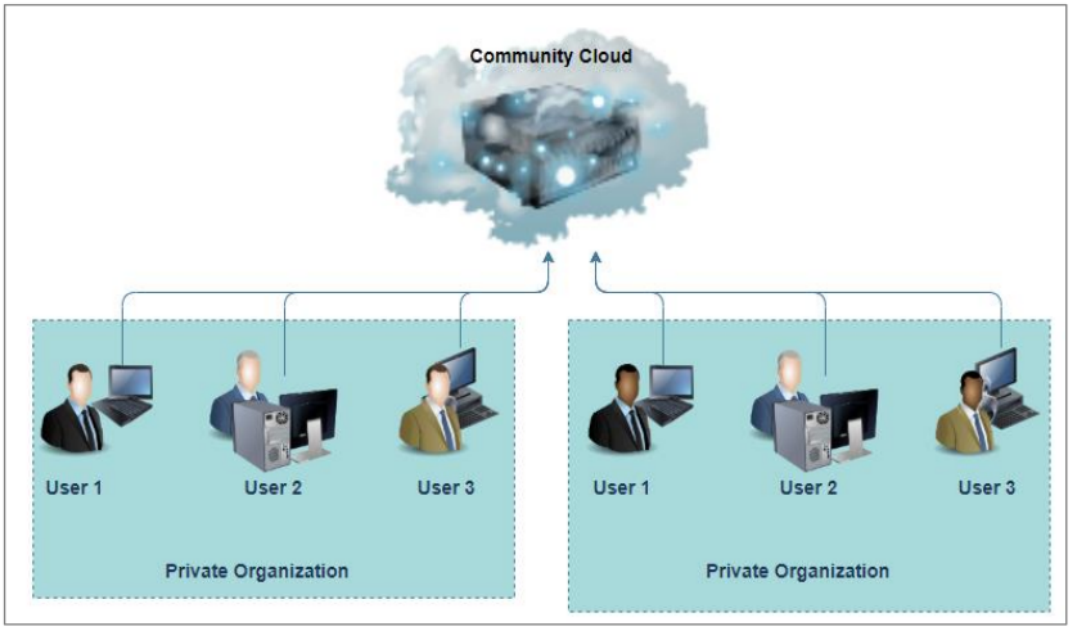

Figure 2.3: Community cloud [21]

d. Hybrid Cloud: A hybrid cloud is, as the name suggests, a combination of two or more cloud platforms. While each hybrid cloud solution differs in performance, they all have the same architecture. Furthermore, as part of the deployment of this cloud computing architecture, internal or external vendors may contribute resources. Let's look at a better example of the hybrid model. Important data should be stored in a private cloud, while less sensitive data should be saved in the public cloud. "Cloud blast" is another term for hybrid cloud. This means that if a business runs an on-premises application, it may burst on the public cloud owing to severe traffic.

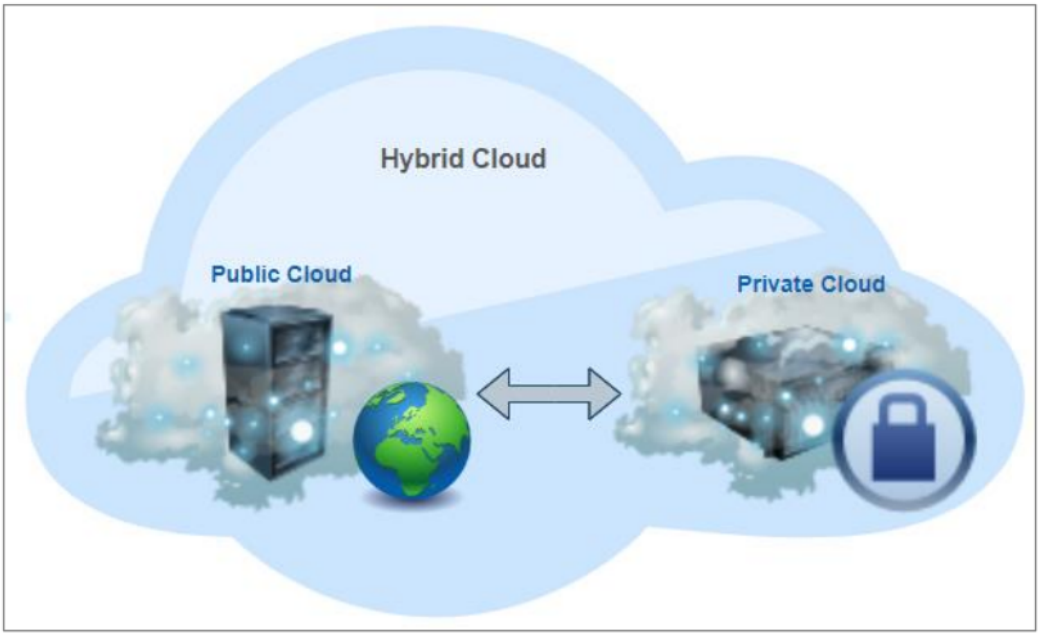

Figure 2.4: Hybrid cloud [22].

A Comparison of Cloud Deployment Methodologies

With the table above, we try to assess the important models and provide an outline about what each one can achieve for you.

Table 2.1: A Comparison of Cloud Deployment Methodologies

Consideration of Important Factors	Public	Private	Community	Hybrid
Setup and usability	Easy	Requires professional IT Team	Requires professional IT Team	Requires professional IT Team
Data Protection and Safety	Low	High	Very High	High
Scalability and adaptability	High	High	Fixed requirements	High
The cost-effectiveness	Most affordable	Most expensive	Cost is distributed among members	Cheaper than private but more expensive than public
Reliability	Low	High	Higher	High

2.2.3 Service Model

Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) are the three primary kinds of cloud service models that cause misunderstanding (SaaS). Let's take a look at each cloud service model individually[23].

a. Infrastructure as a Service (IaaS): Infrastructure as a Service (IaaS) is a method for distant data center infrastructures to self-manage. IaaS (Infrastructure as a Service) is a service that distributes virtualized computing resources via the Internet from a third-party provider such as Amazon Web Services, Microsoft Azure, or Google. Businesses purchase IaaS on a subscription basis rather than purchasing hardware. It's comparable to buying electricity. You just have to pay for the services you use. This approach enables companies to add, remove, or change their IT infrastructure on the fly. Many IT companies choose IaaS because it is more familiar to them, especially if they have years of experience with virtual environments or stringent security and regulatory requirements that can only be met with IaaS.
b. Platform as a Service (PaaS): Platform as a Service (PaaS) enables businesses to develop, deploy, and manage applications without having to invest in IT infrastructure. This makes developing, testing, and deploying apps easier and faster. Developers may concentrate on creating code and developing apps rather than on time-consuming IT infrastructure tasks like server setup, storage, and backup. PaaS increases the value of cloud computing. It can help you save money by lowering your management overhead. PaaS also makes it easy to experiment with new ideas and scale your services on demand.
c. Software as a Service (SaaS): Traditional on-device software is replaced with software that is licensed on a subscription basis using the (SaaS). It is housed in the cloud and is accessible from anywhere. Salesforce.com is a great example. The majority of SaaS programs may be accessed immediately from a web browser, requiring no downloads or installs. Plugins are required for some SaaS apps.

2.2.4 Cloud Architecture

Cloud computing architecture is straightforward; it clearly defines the elements and sub-elements that comprise it. There's little doubt about it: cloud computing is here to remain. It now pervades every aspect of our life, providing several benefits in the form of mobility, storage, collaboration, maintenance, and much more.

Cloud-based software and services such as Google Docs, Skype, and Netflix are accessible via conventional internet access or a virtual network. Most organizations are moving to the cloud because they demand a lot of storage, which cloud applications give. Because a cloud computing architecture gives increased capacity to its users, data stored in the cloud may be accessed at any time from all over the globe. Its architecture allows it to work cooperatively not just with client-side users, but also with fully accessible groups such as Microsoft and Red Hat. The cloud architecture is depicted in Figure 2.5. Depending on the user's access to the cloud, the cloud architecture is separated into four tiers, as follows [24].

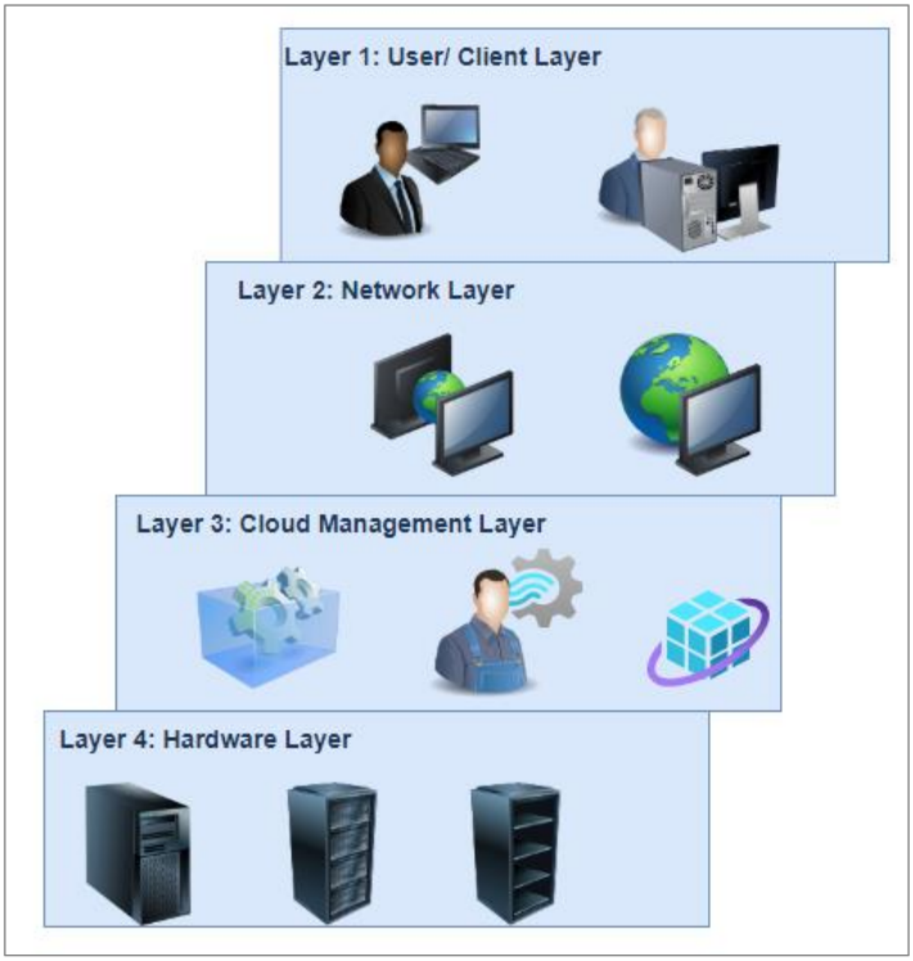

Figure 2.5: Cloud architecture [24]

a. User/Client Layer: This is the lowest layer of the cloud architecture, and it contains all customers or users. In other words, this layer is the point at which the user or client establishes a connection to cloud
b. Computing: It is the network layer that enables users or clients to connect to the cloud. Services are given to clients since the entire cloud architecture is dependent on this connection.
c. Cloud Management Layer: The cloud management layer contains the software required to administer cloud computing. This software might be an operating system, resource management software, or software that acts as a user interface between the data center and the end-user.
d. Hardware Resource Layer: Provisions for genuine hardware resources are included in this layer. In most cases, the data center is used as the back end of public cloud computing. A data center, which is a vast collection of interconnected hardware resources placed in a specified area or highly configured system, can also be a data center in a private cloud. SLAs are responsible for the hardware resource layer. SLAs are governed by this layer, which is the most crucial. When a user uses the cloud, it should be available as soon as feasible and within the timeframes set out in the SLAs. As a result, if a conflict arises in the provision of resources or apps, the cloud service provider will be held liable.

2.3 CLOUD COMPUTING BENEFITS

The following are a few of the many advantages of cloud computing [23]:

a. Achieve Economies of Scale: This refers to raising the amount of output or productivity by utilizing fewer systems, hence lowering project or product expenses per unit.
b. Reduce Spending on Technology Infrastructure: Ease of access to data and information and the least amount of upfront spending through the use of a pay-as-you-go approach. This makes use and payment similar to reading an electricity meter at home, which is based on demand.
c. Workforce Globalization: People from all over the world can access the cloud via an internet connection.

d. Process Simplification: Being able to do more tasks in less time and with fewer resources.
e. Accessibility: Being able to access programs and data from any smart device, at any time, has made our lives much easier.
f. Staff Training Reduce: Working in the cloud requires fewer personnel, while the learning curve for software and hardware issues is reduced.
g. Reduced Software Maintenance and Licensing: Because there are few local computer resources, software system maintenance is cheap, and software system innovations and upgrades are dependent on vendors or cloud providers.
h. Flexibility: In the workplace, adjustments may be made swiftly and without causing major issues.

2.4 CLOUD COMPUTING CHALLENGES

Cloud computing, being a modern tech, has brought several issues in various areas of gathering and analyzing data. The most significant of these problems will be discussed below [25].

a. Confidentiality and Protection: The greatest difficulty to cloud computing is data privacy and security. Cipher, safety devices, and software can be used to address security and privacy challenges.
b. Flexibility: One other cloud computing difficulty is that programs should be readily moved from one cloud provider to another. There should be no proprietary hardware. Unfortunately, it is not yet practicable since each cloud provider's infrastructure employs a separate common language.
c. Interoperability: It indicates that a program on one ecosystem should be able to use capabilities from other companies. It is made feasible through online services, however, implementing such web services is quite difficult.
d. Computing Performance: Information cloud computing services need a large range of network capacity, which comes at a significant cost. Limits the potential does not match the computational quality standards of cloud applications.
e. Accessibility and dependability: Even though most organizations are increasingly reliant on third-party services, cloud solutions must be dependable and resilient.[26].

2.5 CLOUD STORAGE CONCERNS

Both cloud customers and cloud service providers benefit from cloud storage as a service. Cloud customers will be relieved of the obligation for infrastructure upkeep since they will pay the lowest expenses of primary investment. Cloud storage allows users to access cloud services regardless of their location [27].

At the same time, by sharing income with several users, the cloud service provider earns a high return on the available infrastructure. Although using resources at this high level reduces energy consumption, cloud storage has certain inherent flaws, one of which is that it is always presumed that the cloud service provider is untrustworthy and may have harmful intentions. Intentionally (charging all data and deleting data not accessed after analyzing usage statistics or keeping fewer replicas according to commitment) or unintentionally (charging all data and deleting data not accessed after analyzing usage statistics or keeping fewer replicas according to commitment) (the service provider itself does not know if bad sectors have been created in the disk or Hard drive crashes). User concerns concerning cloud storage are listed below [28].

a. Unauthorized Access: Data in cloud computing can be dispersed over several servers and locations. As a result, the user has no control over his data and is unable to preserve it. As a result, one of the drawbacks of cloud storage is the possibility of illegal access. Data breaches can also occur when storage space is repurposed, drives are reused, or equipment is discarded.
b. Espionage of Cloud Provider: Users are hesitant to use cloud storage because they fear that service providers may try to extract sensitive information from their data without their knowledge or consent. Especially when the data contains sensitive information such as credit and bank card details, medical information, and so on.
c. There are no backup services available: Among the most common concerns about storage devices is that they lack automated backup capabilities. They anticipate you to create your

own backups of the data you save on the cloud. To be honest, this isn't a problem with every distribution company; many will continuously back up your data for you. Someone who does not offer copies, on the other hand, does not even have a security net in the case of system failure.

d. Breach of information: Keeping ensuring nobody else in your business attempts to enter your information is a big aspect of safe file storage. A further aspect is ensuring that your information is not shared with anybody beyond your company (unless you send it yourself). Data leaking can be problematic since it exposes sensitive or private information to outside parties. Although if you undertake precautions to avoid data leakage within your company, your hosting supplier may inadvertently reveal your data to someone else.

e. Unwanted gadgets: It's not like every potential threat is posed by the cloud infrastructure. Machines that control your data might potentially be a measure of risk. Several businesses are adopting a bring your own device (BYOD) attitude, which offers many advantages. This indicates that the higher employee machines will have exposure to your cloud infrastructure, which creates a significant potential threat if either of these devices is harmful. Another consideration is dark IT, which refers to any equipment that an employee does not identify but nonetheless utilizes to steal your identity.

f. Storage gateways and APIs: Online storage APIs or memory portals are used by certain businesses to assist them to move their information to the server. Such a process in construction is a go-between for the user and the hosting supplier. They could assist your employees in accessing and managing data on your cloud, but an unsecured API or doorway may lead to severe consequences to your information. If you require or wish to utilize a memory API or portal, be certain it offers trustworthy data encryption.

2.6 CLOUD COMPUTING SECURITY METHOD

Cloud computing has grown so quickly that consumers now store their data on a group of computers managed by the cloud service provider. Users utilize CSP to access or retrieve their data from cloud servers, and they may need to execute dynamic data operations on their data.

However, data security has become a key concern in cloud computing, with confidentiality, integrity, authentication, and availability being the four components of cloud security [29].

a- Data Availability Issue: One of the most significant elements of cloud computing is data availability, which means cloud service providers must ensure that their users can readily access information and applications. According to studies, Amazon's storage services were completely shut down for fewer than five hours in 2014, while Google's storage space was down for less than 15 minutes. As a result, mitigating numerous assaults such as denial of service and guaranteeing system longevity is increasingly crucial to maintaining overall system integrity. To secure the benefit of availability, backup and parallel copying methods, recovery systems, and fault tolerance can be employed [30].

b- The Problem of Data Confidentiality: For safeguarding users' data in the cloud, data confidentiality is critical. Due to the existence of client data across the spread public servers, this is a serious worry in terms of cloud storage. As a result, there is a danger of untrustworthy service providers disclosing private information such as financial data, health records, or personal information from the profile. That implies that all cloud computing service providers and users must keep consumer data private. This is why the data owner encrypts their personal information before transferring it to cloud computing. CSPs and unauthorized users will be unable to see the user's encrypted data as a result of this. The capacity to convert the original information into an unreadable format is the core premise of encryption. [31]. There are two types of encryption algorithms: symmetric or secret key encryption and asymmetric or public-key encryption. In asymmetric cryptography, encryption and decryption are carried out using two separates, but mathematically related keys - often referred to as a public key pair and consisting of a public and private key where the public key is made public and the private key is kept secret. Asymmetric encryption examples include RSA and El Gamal. A symmetric encryption strategy uses the same key to encrypt and decode data. Symmetric encryption schemes include AES, DES, and TEA. The Advanced Encryption Standard (AES) encryption algorithm is one of the most essential in symmetric encryption. AES, also known as Rijndael, is a data encryption method created by the United States National Institute of Standards and Technology (NIST) in 2001. AES

is based on the Rijndael encryption, which was developed by Joan Daemen and Vincent Rijmen, two Belgian cryptographers who submitted a proposal to NIST during the AES selection process. After multiple rounds of screening, AES was found to be more extensively utilized than DES [29]. The AES encryption system is symmetric in that it uses three different key lengths (128 bits, 196 bits, and 256 bits), the packet size is all 128 bits, and the method is quite flexible. As a result, it's widely utilized in both software and hardware. The number of transformation rounds that turn the input, known as plaintext, into the final output, known as ciphertext, is specified by the key size used for an AES encryption. The number of repetition cycles is (10 cycles of repetition for 128-bit keys, 12 cycles of repetition for 192-bit keys and 14 cycles of repetition for 256-bit keys). Each cycle entails certain processing processes, with four stages that are comparable yet distinct, one of which is dependent on the encryption key itself. AES rounds include byte replacement (Sub Bytes), line displacement (Shift Rows), mixed column transformation (Mix Columns), key transformation (Add Round Key), and so on. Using the same encryption key, a set of reverse rounds is used to turn the encrypted text back into plaintext. AES encryption and decryption are seen in Figure 2.6 [28].

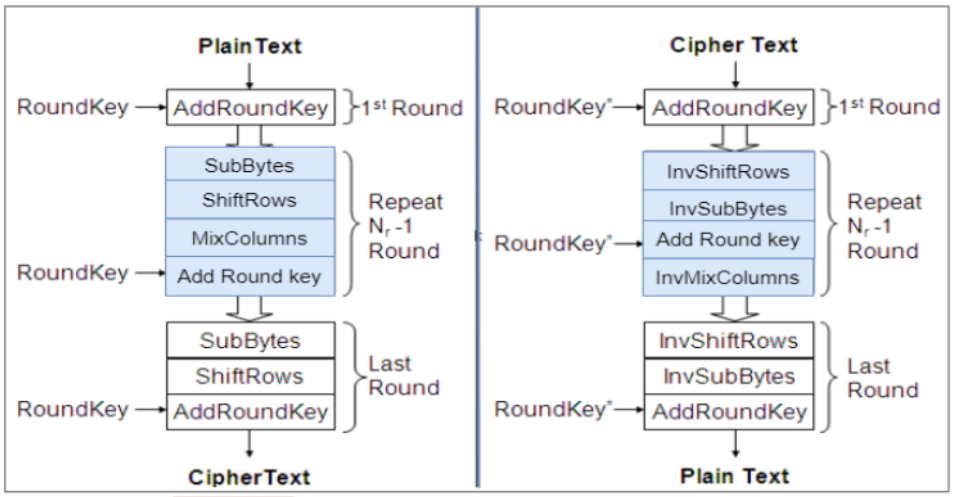

Figure 2.6: AES encryption and decryption [28]

c- The Data Integrity Issue: The mobility of data under the cloud computing concept amplifies the challenges to data integrity. Integrity is described as the protection of data from unauthorized access during the processing, storage, or transport of data, which might occur purposefully or accidentally. Data integrity should be assured within the cloud since data is transported to and from the client and the cloud service provider, as well as internally within the cloud. Several ways exist for ensuring data integrity, including the creation of hashes of stored data and comparing them against newer hashes of the same files. To identify modifications to personal data, cryptographic authentication measures (e.g., message authentication codes or signatures like the BLS signature) are utilized.

The BLS short signature allows a user to verify the credibility of a signer; it is the shortest digital signature and has been shown secure in the random oracle model described by [32]. It was chosen because small signatures are required in cloud situations where bandwidth use must be kept to a bare minimum. When compared to other signatures such as RSA and DSA, the BLS creates short signatures. RSA signatures, for example, are 1024 bits long when using a 1024-bit modulus. Standard DSA signatures are 320 bits long when using a 1024-bit modulus. DSA variations using elliptic curves, such as ECDSA, are similarly 320 bits long. A 320-bit signature is too lengthy for a person to type in. While the BLS signature technique has a length of about 160 bits and gives a degree of security comparable to 320-bit DSA signatures. Signature verification is significantly less computationally demanding than signature production since it contains a computationally unexpansive pairing process. The major advantage of a BLS signature is that it allows you to combine several signatures into numerous messages using various public keys. Key generation, signing, and verification are the three functions of BLS.

a. Key generation: This method generates the private key by selecting a random number $x \in Z_p$ from the range [0, r-1]. The holder of (x) makes the g^x, which represents the public key $\in G_2$.

b. Signing: This function accepts the key (x) and the message (m) and calculates the signature by hashing the (m), for example, h=H(m) ∈ G_1. The signature $S = h^x \in G_1$.is the result of this function. H stands for SHA-256, which is a hash function.

c. Verification: To verify that $e(s, g) = e(H(m), g^x)$you'll need a signature S and the public key g^x. This signature is safe against existential forging under a chosen-message attack since it employs Gap Diffie-Hellman groups (in the random oracle model), The security of the BLS short signature is based on assuming the computational Diffie-Hellman problem (CDH), which is difficult on certain elliptic curves over a finite field but maybe solved cheaply owing to properties like non-degenerate, efficiently calculable, bilinear pairings [18].

Taking (C and CG) as multiplicative cyclic groups of prime order (po) . Therefore ,c represents the producer of C. The map e : C × C→CG will be a bilinear map where the following features are acheived:

a- Calculable: effective process happens of computing map (e);

b- Bilinear: e(ut , vy) = e(u,v)ty for every u; v ∈ C while t; y ∈Gr;

c- Non-degeneracy: e (u,v) guarantees not equal to 1.

Assume that C × C → CG is a non-degenerate, calculable, bilinear, and that (C, CG) are prime order sets. Allow c to be one of the generators. Consider the c, c^x, c^y, case of the computational Diffie-Hellman issue. The computation of c^{xy}, which is the computational Diffie-Hellman problem's resolution, is not aided by the pairing function e. This condition is thought to be intractable. Whether c^z is assumed, the researcher may check to see if $c^z=c^{xy}$ while the values of x, y, and z are unknown, by seeing if $e(c^x,c^y)=e(c,c^z)$ holds. Using the bilinear characteristic x + y + z, the researcher can notice that if $e(c^x,c^y)=e(c,c)^{xy}=e(c,c)^z= e(c,c^z)$, then xy=z. This is because the CG is a prime order set [32].

The BLS signature system uses an incredibly efficient signing algorithm, with just one hashing required to generate a signature. This appears to be the simplest way to create a safe digital signature using rapid hashing.

For data integrity, the BLS signature system employed the SHA256 algorithm. The SHA256 algorithm is a one-way cryptographic hash function that is utilized in both digital certificates and data integrity. NIST is the company that created SHA256. The SHA256 algorithm accepts a message of any length that is less than 264 bits as input and creates a 256-bit message digest of the input [33].

2.7 FEATURES OF DATA INTEGRITY SCHEMES

At this point, we will address the basic concepts of data protection to be able to diagnose and analyze previous work, in addition to developing and improving the main concepts to reach a secure and effective system that aims to ensure the highest data security rate.

a. Public Auditing: Because the cloud provider might well have scarce resources, the independent auditor will be costly, particularly if his information is huge. As a result, the audit process will be transferred to someone else who will be responsible for checking the security of cloud storage.
b. Supporting data dynamics: The data user is constantly trying to provide the most effective cloud storage for their information, then one of the prerequisites for cloud storage performance is the capability for the user to view the saved information and make changes to it. These changes might be deletions, additions, or updates. They must offer a suitable inspection system to enable these dynamic operations and maintain the owner's data secure from manipulation or destruction.
c. Privacy preservation: This indicates that throughout the inspection to assure cloud information integrity, the inspector is incapable of getting original manager's data and information (by utilizing the recovered information of the verified data).
d. Unrestricted Challenge Repetition: This indicates that the number of tests a client or inspector may give to validate the security of cloud environment must be unlimited. It isn't each 0task to verify the security of your cloud service storage data. In order to detect such memory leaks in a timely manner, the user executes the validation method in the interim.

2.8 ANALYSIS OF DATA SECURITY RELATED WORKS

A system has been proposed to enhance private auditing through the permission of users to search for keywords utilizing encrypted dynamic cloud data, which has a symmetric key validation. They devised a novel cumulative authentication signature based on symmetric-key cryptography to construct a cumulative authentication signature for an individual keyword [16]. Devised a zero-knowledge privacy technique to ensure that the third-party auditor knew nothing about client data based on all accessible data. The fundamental drawback of this technique is that it does not allow for simultaneous batch auditing of numerous users [34]. By merging Waters' signature and public auditing of cloud data, developed two ID-based public auditing systems. They proposed a data audit technique for cloud computing based on Merkel's relatively indexed and time-stamped hash. They promised that the external data would not be contaminated, and that they would also restore the final copy of the data [35][36]. This approach allows for auditing of public data as well as dynamic data processing. This approach, however, does not support batch auditing [37]. Proposed a remote data integrity solution based on the algebraic properties of cloud-based external files. They use a table data structure called Divide and Conquer. The disadvantage of this technique is that batch auditing is not supported [38]. suggested a public auditing approach that allows for both block less and batch verification. A doubly linked information table and a location array make up the dynamic structure of this method. As a result, the computational and communication overheads can be drastically minimized. The scheme's inadequacies make privacy protection impossible [39]. Using index logic tables, proposed a dynamic structure and constructed an identity-based non-repudiable dynamic verifiable data possession system for cloud computing. This system fended off a possible attack and avoided the synchronization problem. Furthermore, this system has lower storage and computation costs in dynamic operations. This theme, however, does not meet the definition of the strictest privacy protection model [40].

Suggested an integrity verification scheme for cloud data based on BLS signature, which ensures public auditing while maintaining data privacy. The scheme's drawbacks include the fact that only static data is supported [41]. Developed a strategy to resolve issues about audits. They used a well-known strategy that relied on signatures based on a fuzzy identification.

Although this technique solely considers static data, it ignores data that has been subjected to dynamic actions [42]. Proposed a data integrity checking system based on identity-based aggregate signatures, with a trusted execution environment acting as an auditor to examine the outsourced data on the local side. They also established safe key management in a trusted execution environment, which has now been expanded to handle dynamic data operations fully. They also took into account the circumstance of several file requests for outsourcing occurring at the same time, which can greatly improve the efficiency of integrity checks. With all of these benefits, they decided not to use public auditing and instead replaced the third-party auditor on the client side with a single secure environment [43].

Suggested a dynamic approach for identity-based data auditing for data dynamics. They used Merkle's hash data structure to validate the block tag and therefore assisted to update the data while ensuring integrity in their scheme to perform dynamic operations [44]. Similarly, promoted private auditing by advising that search investigations be done utilizing keywords encrypted dynamic cloud data and symmetric key-based validation. To construct a cumulative authentication tag for each term, they devised a novel cumulative authentication tag based on symmetric key cryptography. The downside of this method is that batch auditing is not supported. Developed a technique to solve this problem [45]. Provided a means of conducting private auditing that involves a cloud data sharing mechanism that applies to mobile devices. Before sharing data with clients, their systems can conduct security tests to ensure that the data is accessible. Their technology also enabled light mobile device operations for the data owner and the one who requests the data. Notwithstanding, their system does not deal with dynamic data operations, contrary to this system [46]. The current study will summarize current solutions and their weaknesses and compare the suggested method in the subsequent sections. Several strategies have recently been addressing the integration and privacy of cloud data. There are some schemes that primarily focus on reading a whole given file to assess its integrity and then derive a total assurance [2]. Advocated for private auditing and offered a cloud-based data sharing mechanism for mobile devices. To prevent wrong computations, their system can guarantee that users have permission to access data by executing security checks before to sharing data with them. Their technique enabled lightweight mobile device operations on both

the data owner and data requester sides. Their technology, on the other hand, didn't handle dynamic data operations or batch auditing. Ping et al., on the other hand [4]. Provided public auditing and used an authenticated data structure called the privacy-preserving adaptive trapdoor hash authentication tree by adding trapdoor hash and BLS signature to the Merkle hash tree. They supported data integrity in their suggested approach, although batch auditing and cloud data confidentiality were not achieved [5]. The public systems that combine TPA with dynamic data facilitate public auditing as proposed in [15]. Also, An Efficient and Secure Auditing System of Cloud Storage has been proposed, it can support auditing and maintains users' privacy based on (BLS) signature, also it supports data dynamic operations [47].

Despite the above basic data integrity standards, previous research has devoted little attention to finding an acceptable approach for this purpose. As such, this thesis pays close attention to these critical aspects of the security of the cloud model and addresses issues related to data privacy and data retention during public scrutiny and confidentiality. Table 2.2 presents the comparison in terms of data integration features between previous systems and our proposed system.

Table 2.2: The comparison between systems

Systems	Public Auditing	Data dynamic	Privacy-preserving	Unrestricted Challenge
[16]	NO	NO	NO	YES
[34]	Yes	Yes	Yes	Yes
[35]	Yes	No	Yes	No
[36]	Yes	No	No	No
[37]	Yes	Yes	No	No
[38]	Yes	Yes	No	No

[39]	Yes	Yes	No	Yes
[40]	No	Yes	Yes	No
[41]	YES	NO	YES	YES
[42]	YES	NO	NO	YES
[43]	No	Yes	Yes	No
[44]	Yes	Yes	Yes	No
[45]	NO	YES	YES	YES
[46]	NO	NO	YES	NO
[2]	YES	YES	NO	YES
[4]	YES	YES	YES	YES
[5]	YES	YES	YES	NO
[15]	NO	NO	YES	YES
[47]	YES	YES	YES	YES
[48]	YES	YES	YES	YES
Our system	YES	YES	YES	YES

3. METHODOLOGY

3.1 INTRODUCTION

Cloud computing brings a slew of appealing features. Cloud storage is one such service, in which the Cloud hosts the client's data and applications. The service is appealing to both businesses and people because of the cost savings and flexibility it provides. Clients, however, have security worries as a result of the service. Because the client's data is kept on Cloud servers, the client loses control over it. Data is vulnerable to a variety of challenges to privacy and integrity, both inside and outside the cloud service provider. To combat these dangers, the client cannot rely solely on the service provider's promise. There is a requirement for more inspections. Data can be transferred and stored in encrypted form to address the privacy problem. Provisions must be created for data integrity verification, ideally by an independent auditor, without jeopardizing the data's privacy to both the Cloud and the Auditor. Over the years, many integrity checking methods have been suggested to assess the integrity of data stored in the Cloud. In these methods, data integrity is checked either by the system administrator or by a third-party auditor hired by the system administrator to certify the data's integrity on their behalf. However, these technologies were unable to discover an integrity solution that met all of the data integrity objectives listed in Chapter Two's examination of relevant work. As a result, this chapter proposes a solution for storing dynamic cloud data using a basic security architecture based on the BLS signature. The suggested system's major goal is to audit cloud data while maintaining privacy on demand without full data recovery or further online burden for cloud users, i.e., The suggested approach allows the TPA to audit customers' cloud computing data without having to study the data's content. In addition, data dynamic operations are supported and enabled. Furthermore, the suggested system uses the AES algorithm to provide data secrecy in cloud storage settings. To secure the proposed method from unauthorized TPA. The suggested solution has been demonstrated to be exceptionally secure after a thorough investigation of security and reliability.

This chapter will present information about the proposed system, as well as the system model and design goals. The specifics of the proposed system are then presented in this chapter.

Furthermore, this chapter discusses the data's dynamic operations and concludes with a summary.

3.2 SYSTEM MODEL

The suggested public auditing system consists of three parts with a clear relationship between them. The proposed data auditing system is illustrated in Figure 3.1.

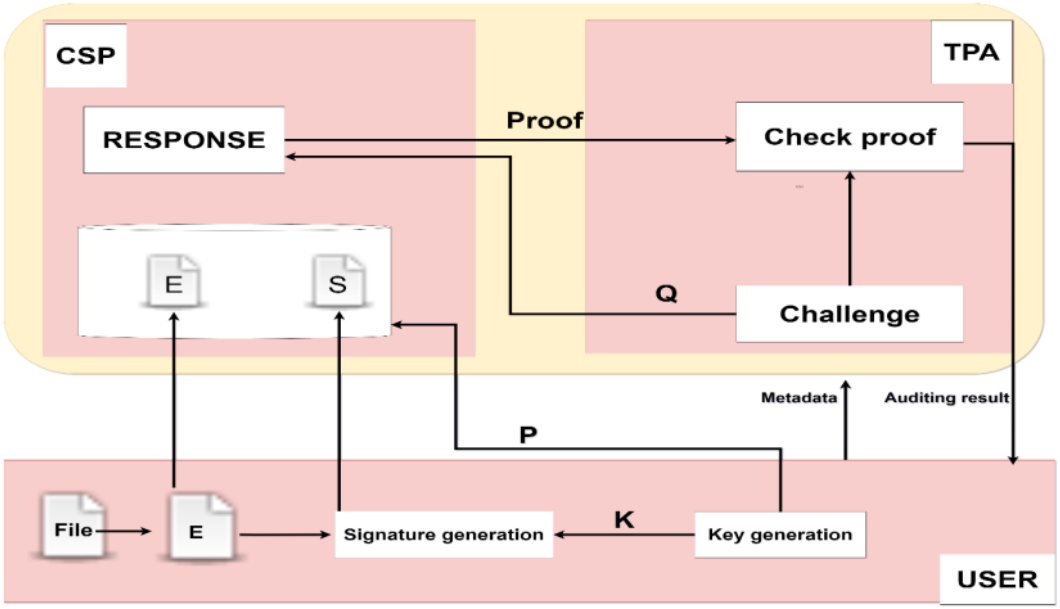

Figure 3.1: The proposed system model

Key letters of figure 3.1:

S: Signature

E: Encrypted files

K: Secret key

P: Public key

Q: Challenge

a. Cloud server: It is controlled by a cloud service provider (CSP) and has the capability (expertise and infrastructure) to host external storage as well as implement adequate solutions for its customers to produce, keep, upgrade, and ask retrieval of information.
b. User(s): Those who have data stored in the cloud delegate IT-related tasks to specialists and focus on their own operations.
c. Third-party auditor (TPA): When appropriate, an extra organization with superior capabilities and expertise is utilized to assess the authenticity and dependability of cloud storage on behalf of consumers.

Users can save money on storage and upkeep by storing large volumes of data in the cloud. The CSP is almost dependable, suggesting that it permits normal data flow through the system. However, the real contents and integrity of the data may not be trusted, which means that the CSP may act unethically against users in regard to the condition of the external data in order to gain advantages. As a result, an integrity checking system must be in place to appropriately store and protect user data. The user can provide TPA permission to undertake out security auditing tasks.

3.3 THREAT MODEL

Assume that having a CSP is virtually completely dependable and that it is operating normally. However, CSP may remove files that are rarely used. Alternatively, the CSP may elect to conceal data corruption in order to protect its reputation. We believe the TPA conducting the audit is independent and trustworthy and thus has no reason to collude with the CSP or the users during the audit process. TPA, on the other hand, can hurt the user if it can learn the data after auditing. As a result, the data integrity employed in a CSP is linked to two categories of risks, which are explained below:

a. Integrity threat: The data, signatures, and public key are all noticed by the attacker. This attacker's goal is to give legitimate evidence of data fraud.
b. Privacy threat: Where the hacker keeps track of information and evidence [59]. This attacker's goal is to learn more about the information, including its substance or kind.

3.4 DESIGN GOALS

The following key aims should be taken into consideration while designing the system:

a. Public auditing: Allows TPA to evaluate cloud data on demand without requiring complete data recovery or adding to cloud customers' online burden.
b. Data confidentiality : To ensure the reliability of the proposed system.
c. Data Integrity Protection: To ensure that the proposed system's data integrity and security are preserved.
d. Privacy-preserving: To guarantee that the audit does not reveal data content to the TPA.
e. Data dynamic support: Even if users update, remove, or insert data into the cloud, the storage accuracy assurance must remain constant.

3.5 THE PROPOSED SYSTEM

The form's user signs in first, then divides the file using a splitting algorithm, and finally encrypts these data blocks using advanced encryption technology (AES 256) [58] to protect the confidentiality of the data, resulting in the encrypted file. For each block of encrypted data, the user generates secret keys, public keys, and signatures before uploading. After transferring the data, signatures, and encryption blocks, the user must erase them from his device. When the client requests that the file be validated, he notifies the TPA service. After that, the TPA is alerted to create assignments and transmit them to the service provider, who then sends them to the user for approval. Once all parties are in agreement, the TPA performs a test to ensure the data's integrity where it sends the results to the client.

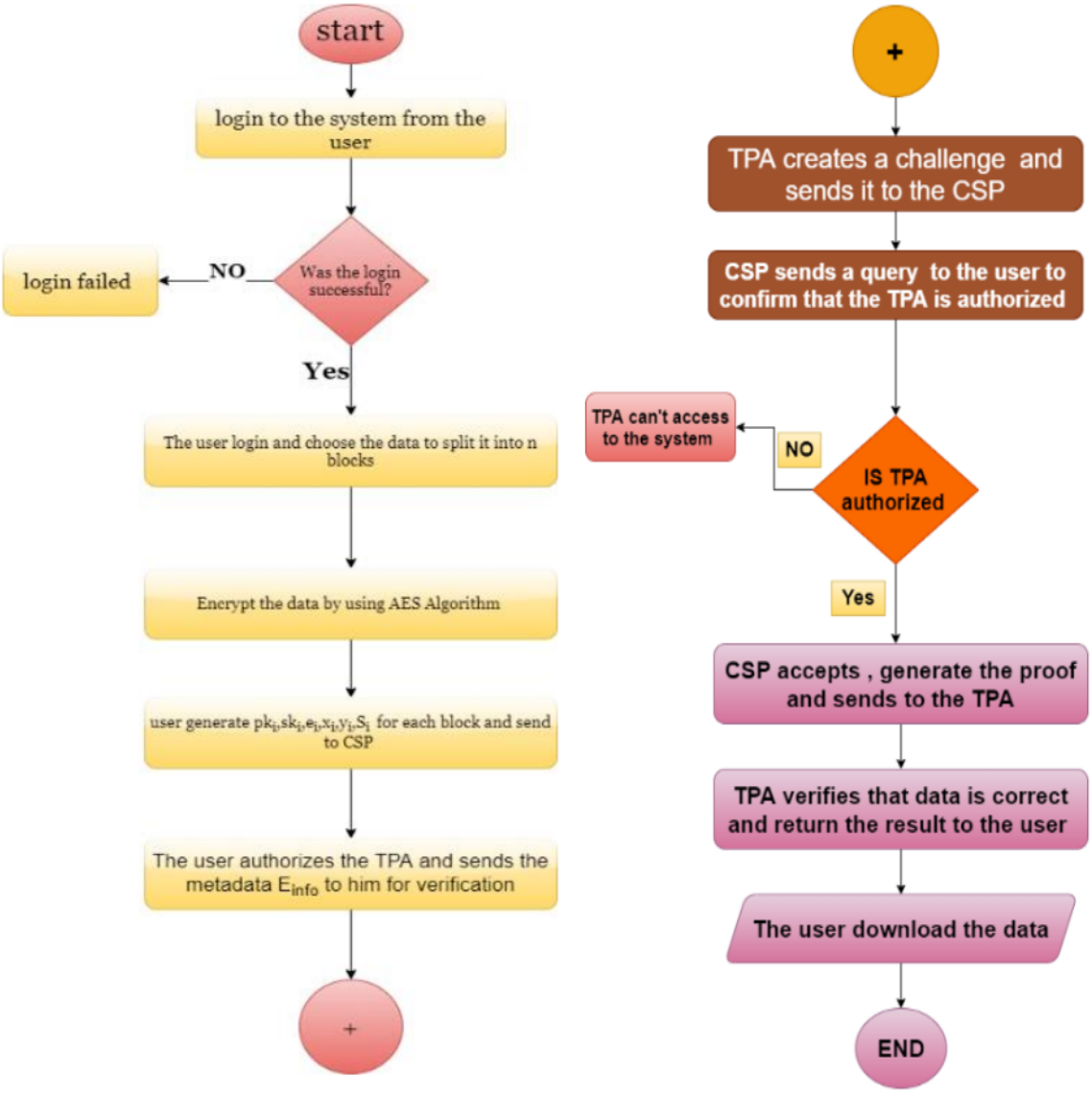

Figure 3.2: User side and cloud side

3.6 PROPOSED SYSTEM

Our proposed system involves the following six steps: Protection of data, keys_generations, Signature_generation, Challenge, Response, and Proof Checking.

a. Protection of data: Data file(DF) will be the input to this function, then the user categorizes the input files to blocks of data using the partition method DF= (df_1,.,df_n) and then encrypts the files using a complex encryption technique called (AES), and these encrypted files are the output for this function.Ec=(ec_1,….,ec_n).

b. Key_generation: The key generation method is used to generate public and secret keys on the user side and choose two random numbers x and y ∈ Gr. The user keeps K and publishes P which is the public key where the researcher reformulate the public key equation to increase its complexity as shown in equation (3.1).This method accepts security parameters k, x and y as inputs (random value) in period [0, r-1] being the secret key K ∈ Gr and (x, y) ∈ Gr it is difficult to predict random values and generates a public key P C for individual blocks.

$$P = (c * (x^y) * K) \qquad (3.1)$$

c. Sign_generation :The signature generation process takes the private key (K) and a random value of (x) and (y) that are added to the signature equation in our proposed system to increase the complexity of the signature equation and the name of the encrypted data file as input and returns the signature for each block, as shown in equation 3.2.

$$S_i = (H(m_i).X^y_i.K_i) \qquad (3.2)$$

The user makes the signatures using the signature generation algorithm, which takes the private key (K) and a random value of (x) and (y) and the hash function of (m) which represents the name of the encrypted data file as input where the output for this function will be a signature for each block of the data. On the other hand, it generates metadata (E_{meta}), which includes block name (m_i). Then, the encrypted data blocks are moved to the cloud storage by the user, together with the accompanying signatures and the public key.

d. Challenge_generation :The challenge generation function is one of the integrity check functions. Where the verification of the data on cloud is required, the third party is used, therefore, a trusted account, TPA is required in the system. This account is activated by the user and sends metadata (E_{meta}) as input for this function to TPA for auditing. To prove file integrity, the TPA communicates with the CSP. To come up with the challenge message

where TPA chooses an element k at random and a subset of Q from set [1, n] and qi ∈Gr from set [1, n]. Assuming Q denotes the set (i, qi), i ∈ Q, the resulting TPA sends Q to CSP.

e. Response :At the time the CSP has obtained a test from the TPA, the client receives a question from the CSP to validate that test, and this cycle to improve the validation of the certified TPA. In the case where the clients consents to the query, the cloud computing service provider acknowledges the request. When the CSP receives the client's acknowledgment, the CSP creates a trustworthiness check for the test, represented by Proof (S_i,P_i). The equation allows us to sum many signs of different squares into one by relying on the features of the computation (BLS) (3.3). The worker then submits an assertion (Proof) to the reviewer for their approval.

$$s = \prod_{I=1}^{k} s_i \qquad (3.3)$$

f. Proof Checking : Finally, when the validator obtains the proof that includes the ends of the equation so that the signature (S) is with an element (c) on the first side of the equation and the public key (P) with the message hash function (H(m)) on the other side of the equation from the CSP, it validates the returned proof using the equation (3.4). It checks the proof, then sends the result to the user whether successful or failed as the case may be.

$$e(S,c) = e(\prod_{i=1}^{k}(H(m_i).P_i)) \qquad (3.4)$$

3.7 SUPPORT OF DATA DYNAMIC OPERATIONS

External data may be accessed and updated often by users in the cloud model for numerous application objectives [1]. As a result, it's critical to enable data dynamics in order to ensure privacy and public auditing. In addition, the research will show how the system handles data dynamics at the block level, such as updates, removals, and insertions.

a. Modification of a data block: In the cloud model, it is one of the most popular procedures for information. This important procedure entails swapping out the required blocks with new ones. Considering the fact that the customer changes block (e_i) to block (e_i). First, the client will send his request to the cloud by means of getting it edited by the block (e_i), then, the

client develops the private and public keys and give new random values (X,Y) to be used in developing the new signature (S_i) (S) for the updated block (e_i) through equation (3.1). Having submitted the request to the cloud computing for the removal of the old block (e_i), with the corresponding values, the metadata of the updated block (E info) is as well updated. This metadata contains (m_i,X^Y_i). At last, the modified block (e_i) is uploaded with the values (S, P) to the cloud, the updated metadata is also transferred to the TPA.

b. Insert data block: In the client encoded data file (Ec) kept on the client, data integration refers to the addition of new consumer blocks after the designated place. Suppose the block will be inserted after the previous one. The customer will select the blocks they wish to add, encrypt it (e_i), construct the secret keys (K and P), and produce the S signature for this block by choosing a random number (x,y). Information (E_{meta}) for it must be created. The user then transmits (E_{meta}) to the TPA, together with the blocks (e_i) and its related values (S_i,P_i).

c. Delete data block: The act of removing a single block from a user file saved in the cloud, after which all following blocks are pushed ahead is the opposite of data insertion. Consequently, if there is any need for removal of the block (e_i), a straight request containing the name of the blocks will be sent to the web server. This requests the deletion of a particular named block (e_i) from the client files including its data (S_i,P_i), and a similar question will be issued to the cloud at the same moment. The blocks name is also included in the TPA. As a result, TPA will erase the blocks name (m_i) from the (e_i) block.

4. RESULTS OF THE PROPOSED SYSTEM

4.1 BERKA DATASET

Petr Berka and Marta Sochorova created the Berka Dataset. Berka is a dataset that contains financial data from a Czech bank. The database includes about 5,300 bank customers and over 1,000,000 transactions. Furthermore, the bank included in the information has granted approximately 700 loans and issued nearly 900 debit cards, all of which are included in the data. Every account has both static (e.g. account id, district id, and frequency) and dynamical (e.g. payments debited or credited, balances) features, which are stated in connection to "permanent order" and "transaction."

4.2 SECURITY ANALYSIS

Security analysis is the most essential metric, it is dependent on the implementation time and is linked to the proposed data auditing system. This paragraph evaluates the recommended system's security analysis based on the proposed system's correctness, token unpredictability, confidentiality, privacy-preserving, and data integrity protection

4.2.1 Unpredictability of Tokens

When generating the signature S for file E, the recommended system creates the random values (x, y). This value is unique to each block, as previously indicated. As a consequence, the attacker was unable to get past the auditing system. The requisite audit can be passed if the cloud server can counterfeit the data's signature. However, the proposed solution requires the server to expect the random value in order to forge the data signature (x, y). Any altered block in the data file will have a new value (x, y). Therefore, the danger will be detected during the audit, demonstrating that the proposed system is safe.

4.2.2 Guarantee of Data Integrity Protection

The common problem is the primary dependence of data integrity protection in the proposed system. Integrity threat is one of the considered threats as an attacker can see public key,

signatures and data. Providing clear evidence of data fraud is the main target of the attack. According to the CDH assumptions, the suggested system ensures cloud data integrity by examining the proposed system's security through a game between challenger and adversary.

4.2.3 Privacy-Preserving Guarantee

This section proves that the proposed system is free of information leakage, ensuring that the attacker is unaware of the audit process. An adversary like TPA is malicious, defiant like a cloud server, trigger this process. To show this, we will conduct the following steps.

a. The opponent chooses random combinations $(m_1, \ldots\ldots, m_k)$, to complete the challenge when he receives metadata $(E_{info} = \quad (m_i))$, from the user

b. For the challenged blocks, the adversary produces a challenge $Q = \{i, q_i\}_{[1 \le i \le k]}$ and sends Q to the challenger seek proof.

c. For the blocks contested, the challenger creates the proof P = (S, PK) and transmits it to the adversary.

Hash (H) is an anti-collision hash function in the proposed signature system. By computing the hash function ($H(m_i)$) for the names of the challenged blocks, by calculating the hash function($H(m_i)$ of the names of the blocks to which it intends to be exposed, an opponent can verify the integrity of the blocks stored in the cloud. After that, the data is validated using equation (3.4), and by signing it, the opponent can be prevented from seeing any information related to the user's data, and this is a guarantee of the success of data privacy.

4.2.4 Confidentiality Guarantee

While working on cloud computing, we must keep in mind the confidentiality and security of user data from other consumers and cloud service providers, and at the same time, the security of the data that is monitored and maintained by the service provider and stored in the cloud is the main concern. To address concerns about secrecy and privacy, the proposed system depends on strong security. When storing and accessing data from the cloud, encryption protects data security. Both plain text and the key should be protected by a more effective encryption mechanism. To ensure data protection, the data file is divided using the splitting algorithm into

a series of data blocks, which are then encrypted using an encryption algorithm AES. We know that the AES key is the same length as the plaintext, indicating that it can withstand a brute force assault, with just one bit of change between the correct and incorrect keys Even when the incorrect key is used, which differs just slightly from the proper key, the original and encrypted data differ dramatically during decryption, according to the findings. Decryption failure can occur if inaccurate data is used, and this will prevent you from recovering the original data. Accordingly, the algorithm is considered sensitive with plain text. As a result, the proposed system ensures security and data confidentiality.

4.2.5 Resistance to Attacks

a- Resistance to Side-Channel Attack in a side-channel attack, hackers and malicious users employ a malicious or unauthorized virtual machine (VM) on the same host to get access to private data. Anyone attempting to access the system in the proposed system is authenticated as a user using the username and password specified by the system administrator. As a result, cloud computing will only provide the necessary data to the trusted user who has been granted permission to interact with the system and do the actions that the user has requested based on his approval of access. As a result, the system is safe from the potential of data theft.

b. Resistance to Malware Injection Attack Malicious users and attackers insert malicious scripts into cloud computing servers, and when that code is executed, they have access to private information stored on cloud computing servers. This type of injection can go undetected for a long time, which is why it's so important in the cloud. The data owner encrypts the data using AES in the proposed manner, which means that the data is stored in an encrypted form on the cloud. Therefore, even if the attacker injects malware to access the data, it will not be able to decrypt the content of the data. Accordingly, the proposed system is considered secure against this attack. Therefore, the proposed system is immune to privacy threat.

c. Resistance to Integrity Attack one of the risks we assess is an integrity attack, where an attacker verifies the public key, data, and signatures. The main reason for this attack is to

establish valid proof of data tampering. In the suggested system we ensure the integrity of cloud data while protecting it based on assumptions by analyzing the security of the recommended system in a game between challenger and adversary, as described in subsection (4.2.2).

4.3 ANALYSIS THE PERFORMANCE

Another important performance metric is the evaluation of the proposed framework's productivity with respect to execution testing, so the researcher can demonstrate the framework's existence on all sides, including the client, evaluator, and cloud expert organization sides. In this section, the researcher will evaluate our suggested framework's exhibition in terms of correspondence and calculation costs, as:

a- Computation cost: expenses attached to manufacturing keys and markings, as well as the cost of the client transferring & downloading message blocks from cloud, the cost of the CSP doing the verification, and the cost of the TPA evaluating the proof.

b- Communication cost: The magnitude of the data transmitted by the TPA in the correspondence between the TPA & the CSP.

The suggested scheme is executed in Python using runs on Intel (R) Core i7 CPU, memory size of 1.90 GHz & 8.00 GB RAM. The Berka dataset is used to check for the presence of the suggested framework. The Berka dataset is assembled as a set of financial data from a bank in Czech Republic. In terms of putting the suggested framework into action and evaluating its capabilities, the researcher relies on the informative index for the first document, so the client divides the record into a bunch of squares ranging from (100 squares) to (500 squares), with the square size in our tests being (1 kilobyte). In addition, the researcher used the Drop-box cloud framework to deliver our data and evaluate the suggested framework.

4.3.1 Computation cost

The client-side, TPA-side, & CSP-side computing costs of the proposed framework are calculated. So, the suggested framework's execution is tested in all of its nuances in order to ensure security & productivity using the given calculations.

Figure. 4.1 displays the split information with the varied amounts of the information block on the client side. Figure 4.1 shows that dividing the data of 100 squares of the proposed framework takes less than 0.2 seconds. Following the division of data into a few squares, these squares are encoded with the AES algorithm to ensure categorization. In comparison to [47], Figure. 4.2 depicts the computational cost of client-side encoding with various quantities of suggested framework information content, also we have compared our results with them and shows better performance than them[47][49]. According to Figure. 4.2, the suggested framework takes less than 0.20 seconds to encode 500 KB of data, whereas takes 0.57 seconds. Along these lines, the suggested framework's crypto cost is still

appealing since it increases information security for re-appropriating and does not deserve the client's assets, with reduced computational costs, ensuring the proposed framework's productivity.

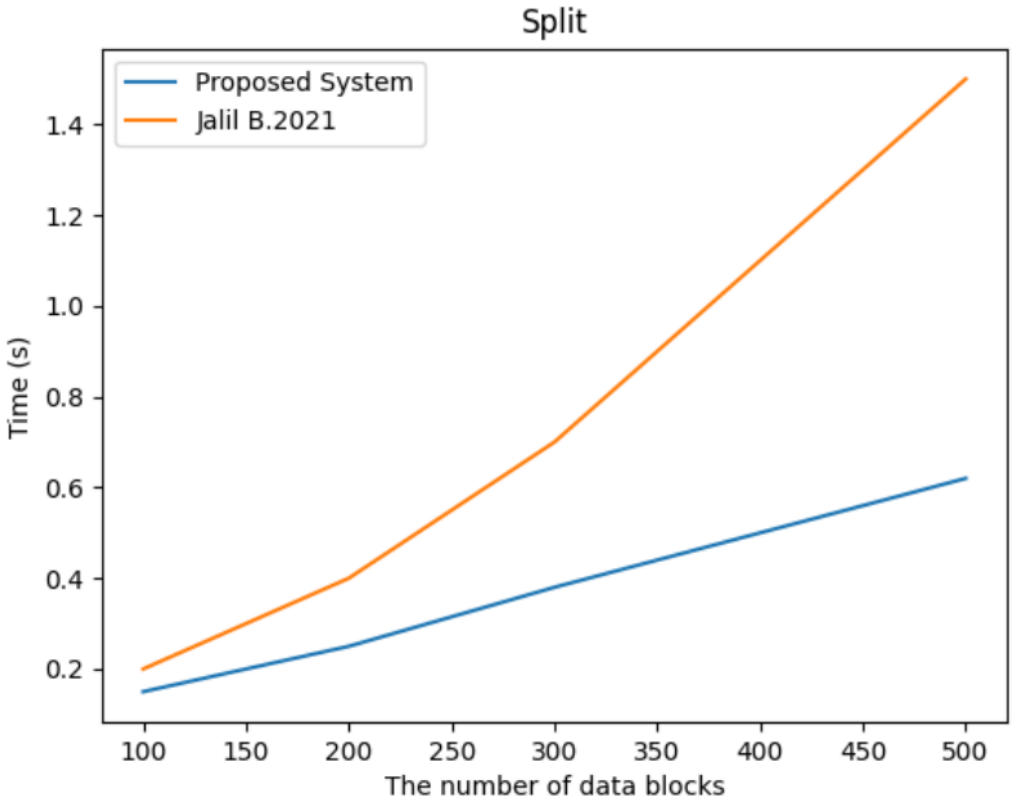

Figure 4.1: The cost of split data computation.

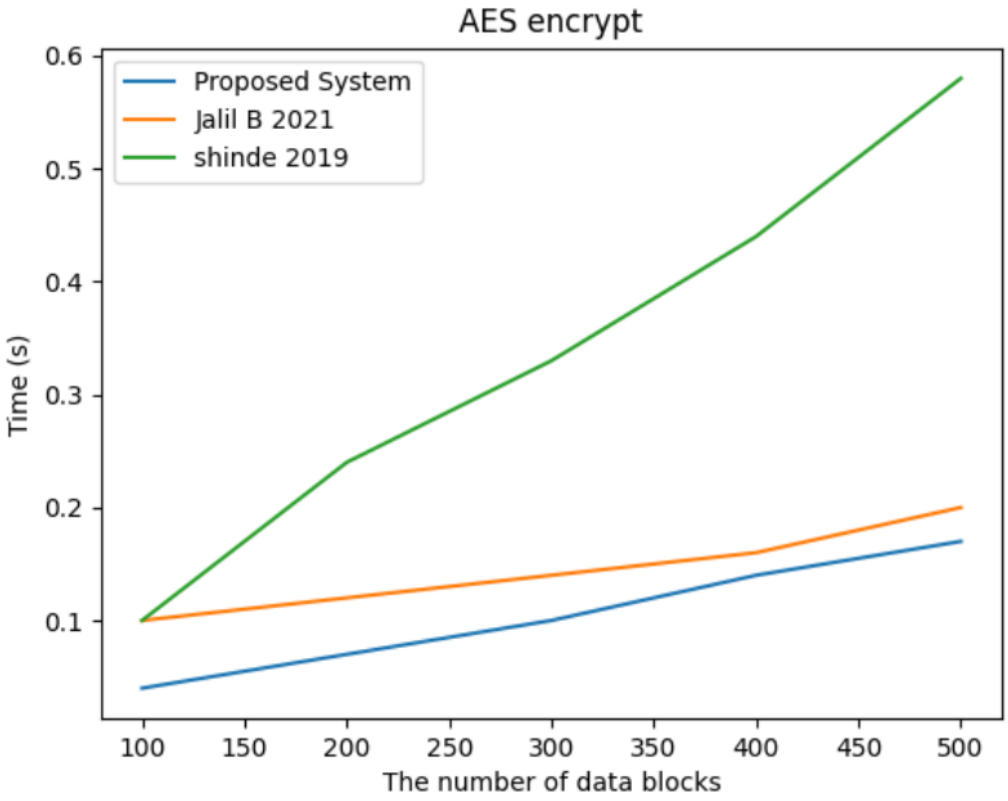

Figure 4.2: The cost of encryption computation

The client then outputs the keys and markings, showing that the time will be fast when he chooses (100) blocks, taking only 0.002 seconds. Signature age, on the other hand, takes longer per square of data. 0.001 seconds is the cost of providing marks for 100 square information documents. On the other hand, the suggested framework examines the actual age and markings by increasing the document size from 100 to 500 squares and documenting the hour of the cycle. They often increase proportionally to the document size when they are examined to deliver scores for a particular record. Figures 4.3 and 4.4 show the nuances of the keys and markings created.

The proposed remote data integrity system is compared to the existing systems in terms of server & auditor computation in the figures 4.3 and 4.4 [47][48]. The proposed scheme performed better than the existing systems and is more appropriate for verifying the integrity of the dataset during both auditor and server computations.

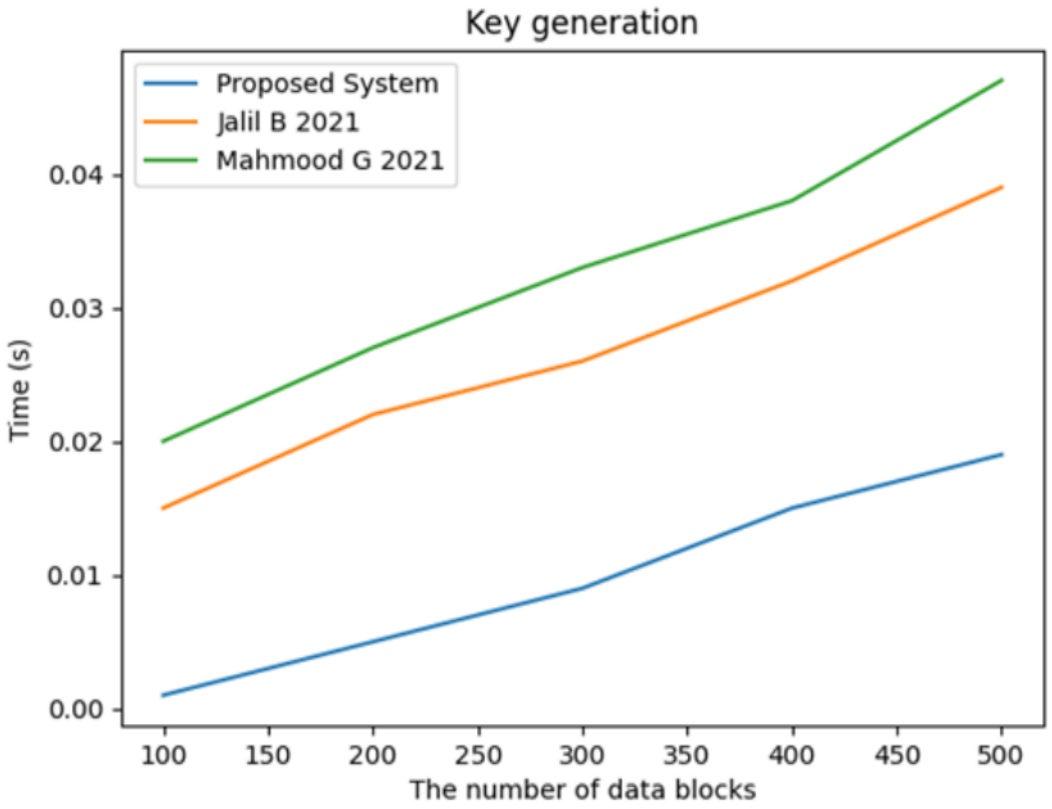

Figure 4.3: Keys generation time

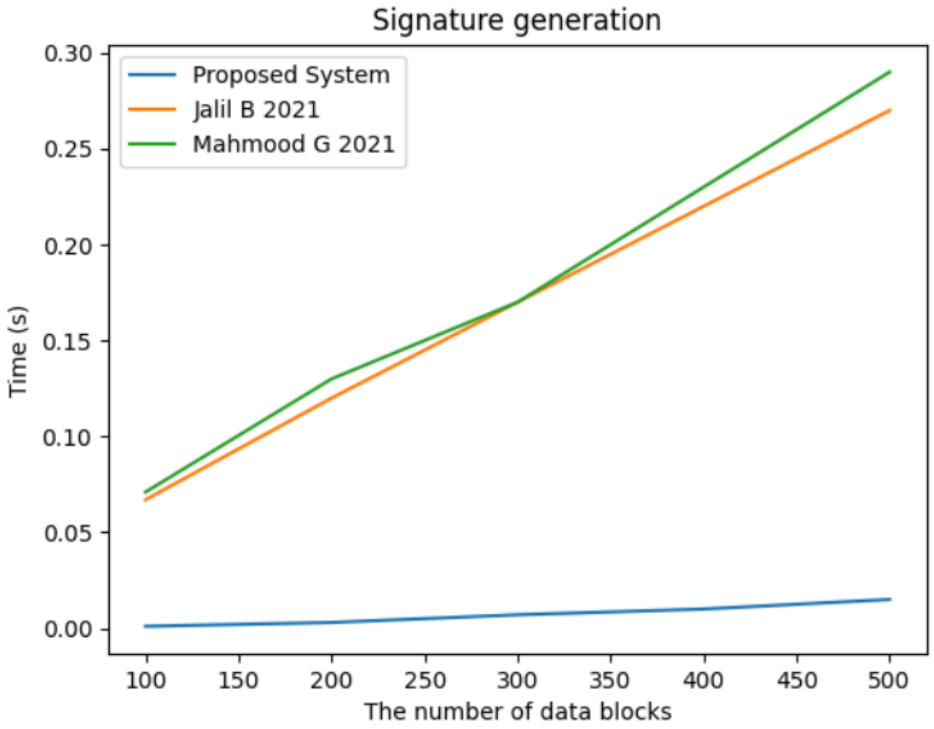

Figure 4.4: Signatures generation time.

However, it generates work for the auditor coupled with the audit technique. Meanwhile, the proof-creation procedure is completely server-based. It's worth noting that setting up a challenge for 100 KB takes only 0.028 seconds. Reaction and editing, on the other hand, are more time consuming. To see how much time, it took to set up a challenge, answer it, and proof it, the number of challenges is increased from 100 to 500. As shown in Figures 4.5 and 4.6, the time it took to set up a challenge, answer it, and proof it increased as the number of challenges increased. The rising number of challenged blocks necessitates the use of random values in producing the challenges, and since there are more computations in the cloud and more operations on the auditor's side, this is suited for experimental research.

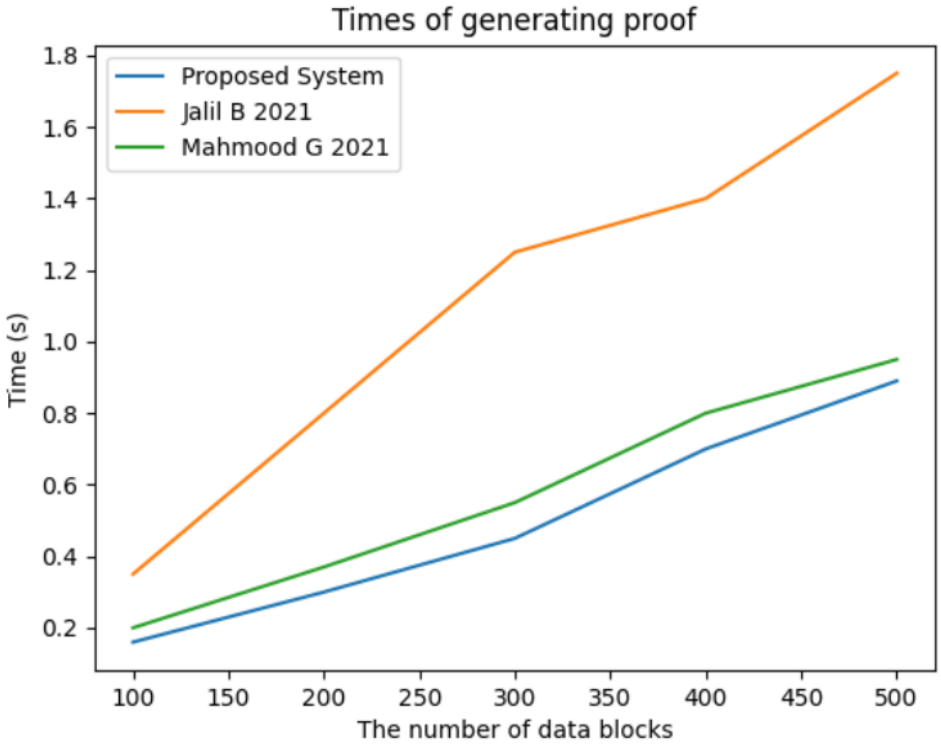

Figure 4.5: Proof-generating times

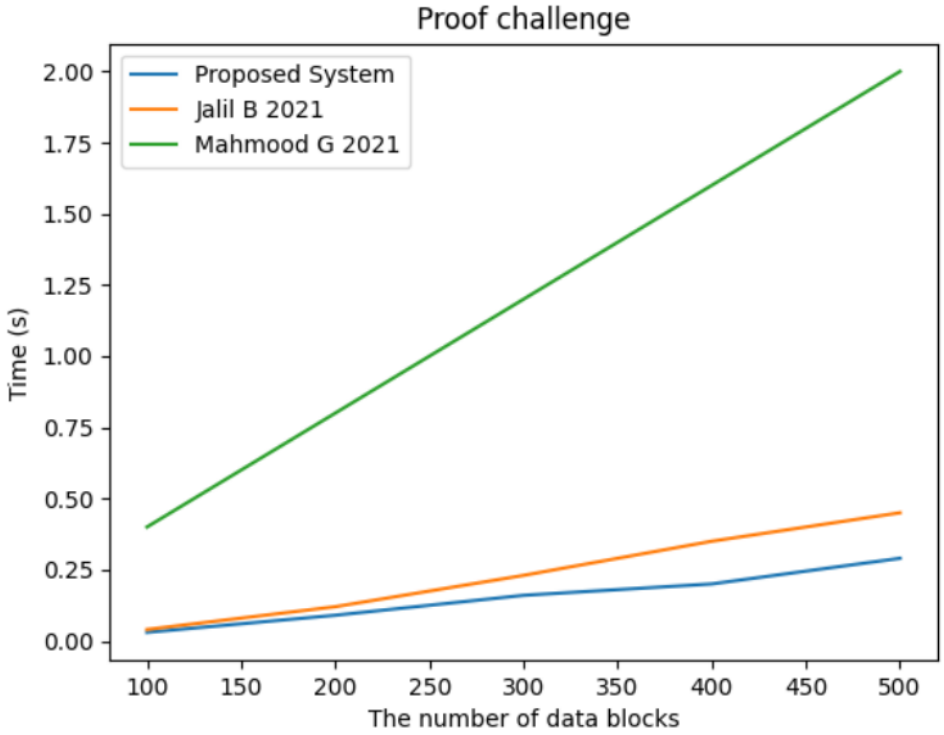

Figure 4.6: Time to create the challenge and verify the proof

Lastly, once the blocks have been downloaded from the cloud, the user must decrypt the blocks before the original data file can be retrieved by combining the resulting blocks. According to Figure. 4.7, about 0.2 seconds is needed to decrypt 500 KB into the suggested scheme, whereas decrypting the data takes 1.09 seconds[47] [48]. As a consequence, the recommended technique has a low computational cost for decrypting data. Figure 4.8 shows how to generate the original data file by joining the blocks collected during the decoding process.

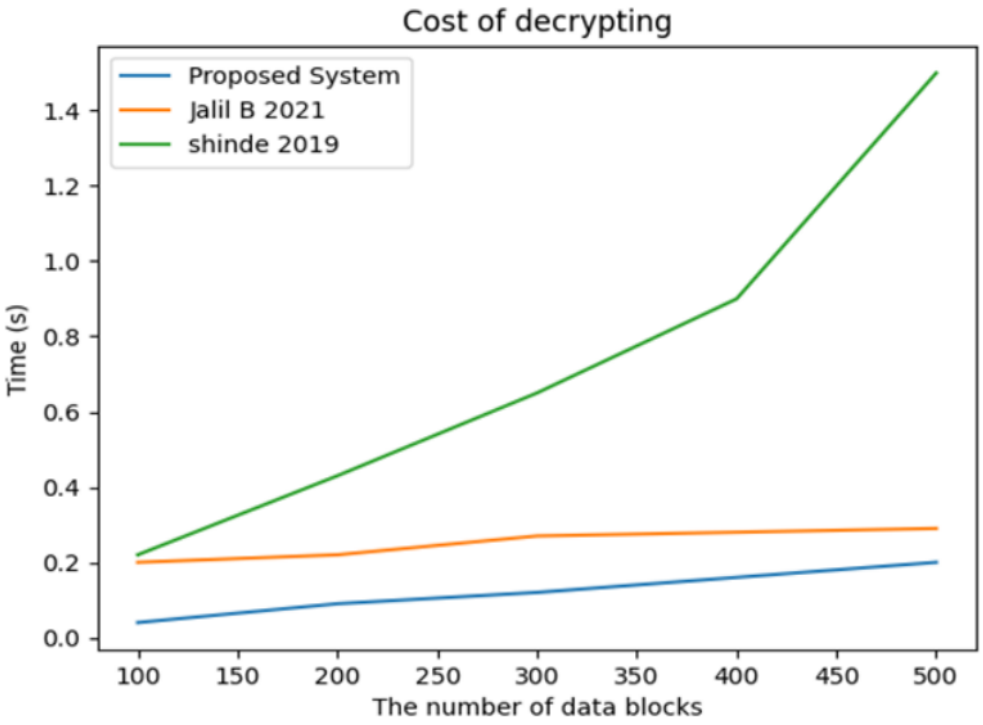

Figure 4.7: The cost of decryption computation.

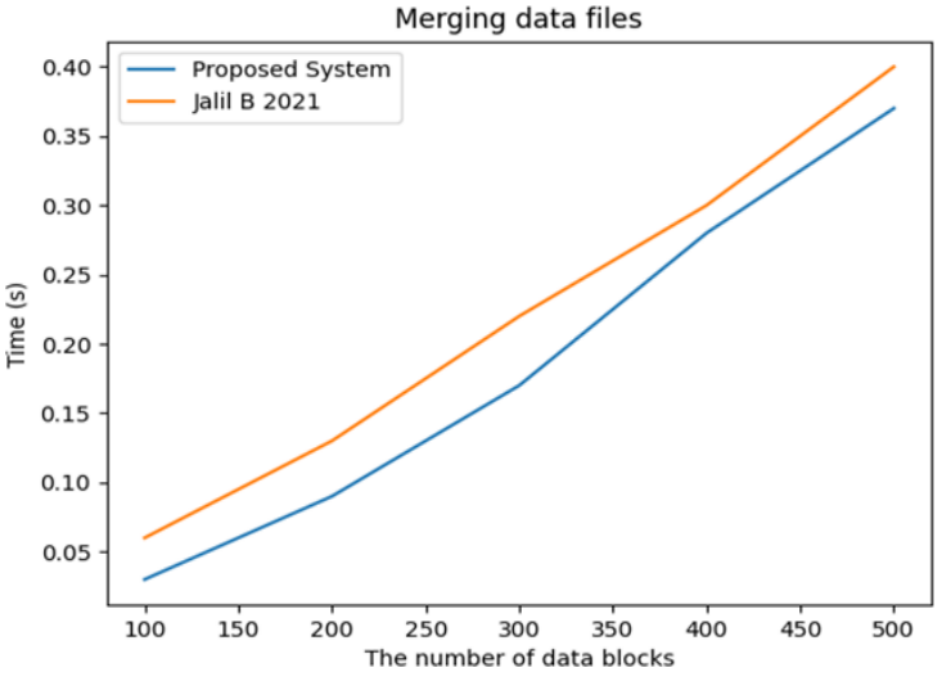

Figure 4.8: The computational cost of combining blocks

4.3.2 Communication cost

The costs of connection are involved in the processes of publishing "data to the cloud," obtaining the same information to the cloud, and reacting to auditing difficulties. During audit operations, the cost for challenge blocks, denoted as Q (i,qi) in the challenging section, is a function of the blocks n given by TPA for the audit; hence, the proposed system is outfitted with random blocks decided by TPA to challenge (n).Several tests are carried out in order to assess how long it takes to upload and retrieve data from the cloud utilizing the suggested approach. The encrypted blocks are transferred to the cloud after splitting the data file into numerous parts and encrypting the resultant data blocks. As a result, Figures 4.9 and 4.10 demonstrate the effects of uploading and downloading." The average communication time stays constant with small block sizes, as seen in Figures. 4.9 and 4.10. This weight, on the other hand, is increasing. The researcher also concludes that uploading data blocks requires less time than retrieving them. As a consequence,

it is discovered that the time necessary to transmit and the blocks download from the cloud is proportional to the total blocks involved. 11." In response to variations of information, the transmission time to transmit a fresh block of 500 KB to the cloud is around 0.38 sec, while the download time is approximately 0.13 sec.

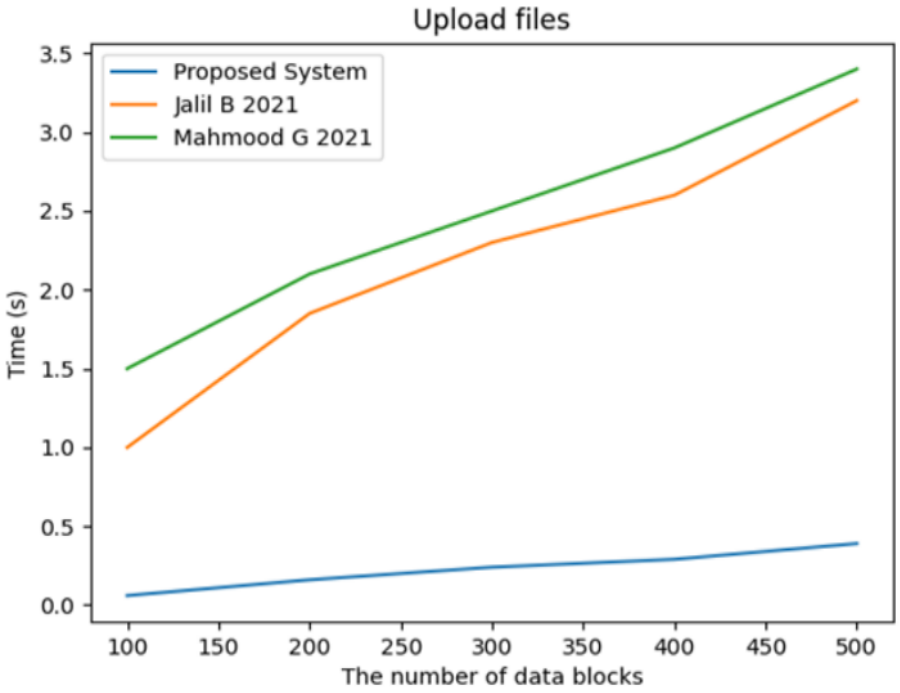

Figure 4.9: The upload blocks

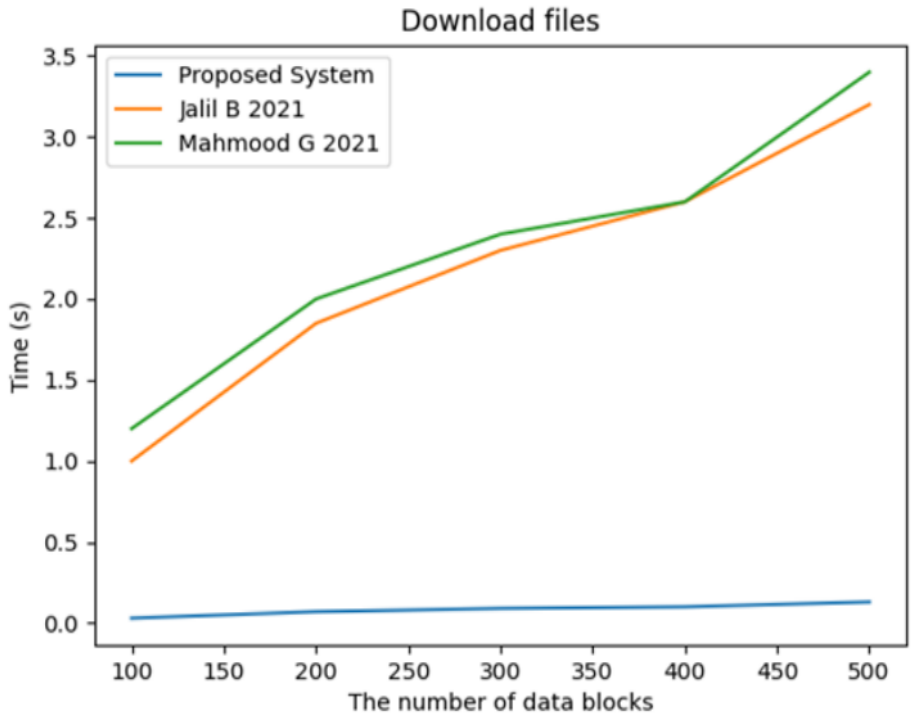

Figure 4.10: The download blocks

5. CONCLUSION AND FUTURE WORK

5.1 CONCLUSION

An audit method based on the signature (BLS) has been developed to protect data kept in the cloud. The proposed system has provided strong data secrecy by encrypting it before uploading it to the cloud. Dynamic data operations, including insertion, deletion, and modification, are also available. Because signature authentication requires only one component, the researcher explicitly proves that the calculation cost of ensuring data integrity is low for the auditing task. As a result, the cost of storing and transmitting signatures can be reduced. According to the detailed analysis, the proposed system is incredibly efficient and secure. For the successful analysis of the system's effectiveness, its performance is compared to that of other systems. The results reveal that the proposed system is simple in computing and communication. The researcher has noticed how this system is set up to be very efficient in maintaining the confidentiality of the database scheme used and on which he ran this test.

5.2 FUTURE WORK

As a future work, we expect the system to develop further to include processing huge data on the largest cloud computing services, and to maintain the security of this data and its effective auditing, while maintaining speed in implementation and performance.

REFERENCES

[1] H. Tian, F. Nan, H. Jiang, C. C. Chang, J. Ning, and Y. Huang, "Public auditing for shared cloud data with efficient and secure group management," *Information Sciences*, vol. 472, pp. 107–125, Jan. 2019, doi: 10.1016/J.INS.2018.09.009.

[2] N. Garg, S. Bawa, and N. Kumar, "An efficient data integrity auditing protocol for cloud computing," *Future Generation Computer Systems*, vol. 109, pp. 306–316, Aug. 2020, doi: 10.1016/J.FUTURE.2020.03.032.

[3] A. Alrabea, "A modified Boneh-Lynn-Shacham signing dynamic auditing in cloud computing," *Journal of King Saud University - Computer and Information Sciences*, Jun. 2020, doi: 10.1016/J.JKSUCI.2020.06.001.

[4] Y. Ping, Y. Zhan, K. Lu, and B. Wang, "Public Data Integrity Verification Scheme for Secure Cloud Storage," *Information 2020, Vol. 11, Page 409*, vol. 11, no. 9, p. 409, Aug. 2020, doi: 10.3390/INFO11090409.

[5] Y. Sun, Q. Liu, X. Chen, and X. Du, "An Adaptive Authenticated Data Structure with Privacy-Preserving for Big Data Stream in Cloud," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3295–3310, 2020, doi: 10.1109/TIFS.2020.2986879.

[6] J. Tian and X. Jing, "Cloud data integrity verification scheme for associated tags," *Computers & Security*, vol. 95, p. 101847, Aug. 2020, doi: 10.1016/J.COSE.2020.101847.

[7] J. Li, J. Wu, G. Jiang, and T. Srikanthan, "Blockchain-based public auditing for big data in cloud storage," *Information Processing & Management*, vol. 57, no. 6, p. 102382, Nov. 2020, doi: 10.1016/J.IPM.2020.102382.

[8] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in*

Bioinformatics), vol. 5789 LNCS, pp. 355–370, 2009, doi: 10.1007/978-3-642-04444-1_22.

[9] Q. Zhao, S. Chen, Z. Liu, T. Baker, and Y. Zhang, "Blockchain-based privacy-preserving remote data integrity checking scheme for IoT information systems," *Information Processing & Management*, vol. 57, no. 6, p. 102355, Nov. 2020, doi: 10.1016/J.IPM.2020.102355.

[10] L. Sun, C. Xu, Y. Zhang, and K. Chen, "An efficient iO -based data integrity verification scheme for cloud storage," *Science China Information Sciences*, vol. 62, no. 5. Science in China Press, May 01, 2019. doi: 10.1007/s11432-018-9500-0.

[11] W. Shen, J. Qin, J. Yu, R. Hao, and J. Hu, "Enabling Identity-Based Integrity Auditing and Data Sharing with Sensitive Information Hiding for Secure Cloud Storage," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 2, pp. 331–346, Feb. 2018, doi: 10.1109/TIFS.2018.2850312.

[12] B. Shao and Y. Ji, "Efficient TPA-based auditing scheme for secure cloud storage," *Cluster Computing*, vol. 24, no. 3, pp. 1989–2000, Sep. 2021, doi: 10.1007/S10586-021-03239-X/FIGURES/4.

[13] H. Shacham and B. Waters, "Compact Proofs of Retrievability," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 5350 LNCS, pp. 90–107, 2008, doi: 10.1007/978-3-540-89255-7_7.

[14] G. Ateniese *et al*., "Provable data possession at untrusted stores," *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 598–610, 2007, doi: 10.1145/1315245.1315318.

[15] X. Lu, Z. Pan, and H. Xian, "An efficient and secure data sharing scheme for mobile devices in cloud computing," *Journal of Cloud Computing*, vol. 9, no. 1, pp. 1–13, Dec. 2020, doi: 10.1186/S13677-020-00207-5/FIGURES/9.

[16] ErwayC. Chris, KüpçüAlptekin, PapamanthouCharalampos, and TamassiaRoberto, "Dynamic Provable Data Possession," *ACM Transactions on Information and System Security (TISSEC)*, vol. 17, no. 4, Apr. 2015, doi: 10.1145/2699909.

[17] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 5, pp. 847–859, 2011, doi: 10.1109/TPDS.2010.183.

[18] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," *Proceedings - IEEE INFOCOM*, 2010, doi: 10.1109/INFCOM.2010.5462173.

[19] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," *Proceedings - IEEE INFOCOM*, 2010, doi: 10.1109/INFCOM.2010.5462173.

[20] P. Mell and T. Grance, "The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology."

[21] A. Sunyaev, "Fog and Edge Computing," *Internet Computing*, pp. 237–264, 2020, doi: 10.1007/978-3-030-34957-8_8.

[22] T. Vasiljeva, S. Shaikhulina, and K. Kreslins, "Cloud Computing: Business Perspectives, Benefits and Challenges for Small and Medium Enterprises (Case of Latvia)," *Procedia Engineering*, vol. 178, pp. 443–451, Jan. 2017, doi: 10.1016/J.PROENG.2017.01.087.

[23] P. Dašić, J. Dašić, and B. Crvenković, "Service models for cloud computing: Search as a service (SaaS)," *International Journal of Engineering and Technology*, vol. 8, no. 5, pp. 2366–2373, 2016, doi: 10.21817/ijet/2016/v8i5/160805034.

[24] I. Odun-Ayo, M. Ananya, F. Agono, and R. Goddy-Worlu, "Cloud Computing Architecture: A Critical Analysis," *Proceedings of the 2018 18th International Conference on Computational Science and Its Applications, ICCSA 2018*, Aug. 2018, doi: 10.1109/ICCSA.2018.8439638.

[25] M. K. Sinchana and R. M. Savithramma, "Survey on Cloud Computing Security," *Lecture Notes in Networks and Systems*, vol. 103, pp. 1–6, 2020, doi: 10.1007/978-981-15-2043-3_1/COVER/.

[26] L. B. Bhajantri and T. Mujawar, "A Survey of Cloud Computing Security Challenges, Issues and their Countermeasures," *Proceedings of the 3rd International Conference on I-SMAC IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2019*, pp. 376–380, Dec. 2019, doi: 10.1109/I-SMAC47947.2019.9032545.

[27] L. Wei *et al*., "Security and privacy for storage and computation in cloud computing," *Information Sciences*, vol. 258, pp. 371–386, Feb. 2014, doi: 10.1016/J.INS.2013.04.028.

[28] P. R. Kumar, P. H. Raj, and P. Jelciana, "Exploring Data Security Issues and Solutions in Cloud Computing," in *Procedia Computer Science*, 2018, vol. 125, pp. 691–697. doi: 10.1016/j.procs.2017.12.089.

[29] A. Mondal, S. Paul, R. T. Goswami, and S. Nath, "Cloud computing security issues challenges: A Review," *2020 International Conference on Computer Communication and Informatics, ICCCI 2020*, Jan. 2020, doi: 10.1109/ICCCI48352.2020.9104155.

[30] W. Guo *et al*., "Improved Proofs Of Retrievability And Replication For Data Availability In Cloud Storage," *The Computer Journal*, vol. 63, no. 8, pp. 1216–1230, Aug. 2020, doi: 10.1093/COMJNL/BXZ151.

[31] K. Suresha and P. Vijaya Karthick, "Enhancing data security in cloud computing using threshold cryptography technique," *Lecture Notes in Electrical Engineering*, vol. 643, pp. 231–242, 2020, doi: 10.1007/978-981-15-3125-5_25/COVER/.

[32] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from the Weil Pairing," *Journal of Cryptology 2004 17:4*, vol. 17, no. 4, pp. 297–319, Jul. 2004, doi: 10.1007/S00145-004-0314-9.

[33] M. Husni *et al*., "Security audit in cloud-based server by using encrypted data AES -256 and SHA-256," *IOP Conference Series: Materials Science and Engineering*, vol. 830, no. 3, p. 032015, Apr. 2020, doi: 10.1088/1757-899X/830/3/032015.

[34] Y. Yu *et al*., "Enhanced privacy of a remote data integrity-checking protocol for secure cloud storage," *International Journal of Information Security*, vol. 14, no. 4, pp. 307–318, Aug. 2015, doi: 10.1007/S10207-014-0263-8/FIGURES/6.

[35] Y. Yu *et al*., "Identity-Based Remote Data Integrity Checking with Perfect Data Privacy Preserving for Cloud Storage," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 4, pp. 767–778, Apr. 2017, doi: 10.1109/TIFS.2016.2615853.

[36] J. Zhang and Q. Dong, "Efficient ID-based public auditing for the outsourced data in cloud storage," *Information Sciences*, vol. 343–344, pp. 1–14, May 2016, doi: 10.1016/J.INS.2015.12.043.

[37] N. Garg and S. Bawa, "RITS-MHT: Relative indexed and time stamped Merkle hash tree based data auditing protocol for cloud computing," *Journal of Network and Computer Applications*, vol. 84, pp. 1–13, Apr. 2017, doi: 10.1016/J.JNCA.2017.02.005.

[38] M. Sookhak, F. Richard Yu, and A. Y. Zomaya, "Auditing Big Data Storage in Cloud Computing Using Divide and Conquer Tables," *IEEE Transactions on Parallel and Distributed Systems*, vol. 29, no. 5, pp. 999–1012, May 2018, doi: 10.1109/TPDS.2017.2784423.

[39] J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, "An Efficient Public Auditing Protocol with Novel Dynamic Structure for Cloud Data," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 10, pp. 2402–2415, Oct. 2017, doi: 10.1109/TIFS.2017.2705620.

[40] F. Wang, L. Xu, H. Wang, and Z. Chen, "Identity-based non-repudiable dynamic provable data possession in cloud storage," *Computers & Electrical Engineering*, vol. 69, pp. 521–533, Jul. 2018, doi: 10.1016/J.COMPELECENG.2017.09.025.

[41] X. Luo, Z. Zhou, L. Zhong, J. Mao, and C. Chen, “An Effective Integrity Verification Scheme of Cloud Data Based on BLS Signature,” *Security and Communication Networks*, vol. 2018, 2018, doi: 10.1155/2018/2615249.

[42] W. Shen, J. Qin, J. Yu, R. Hao, J. Hu, and J. Ma, “Data Integrity Auditing without Private Key Storage for Secure Cloud Storage,” *IEEE Transactions on Cloud Computing*, pp. 1–1, Jun. 2019, doi: 10.1109/TCC.2019.2921553.

[43] Y. Fan, X. Lin, G. Tan, Y. Zhang, W. Dong, and J. Lei, “One secure data integrity verification scheme for cloud storage,” *Future Generation Computer Systems*, vol. 96, pp. 376–385, Jul. 2019, doi: 10.1016/J.FUTURE.2019.01.054.

[44] T. Shang, F. Zhang, X. Chen, J. Liu, and X. Lu, “Identity-Based Dynamic Data Auditing for Big Data Storage,” *IEEE Transactions on Big Data*, pp. 1–1, Sep. 2019, doi: 10.1109/TBDATA.2019.2941882.

[45] X. Ge *et al*., “Towards Achieving Keyword Search over Dynamic Encrypted Cloud Data with Symmetric-Key Based Verification,” *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 1, pp. 490–504, Jan. 2021, doi: 10.1109/TDSC.2019.2896258.

[46] G. S. Mahmood and D. J. Huang, “PSO-based Steganography Scheme Using DWT-SVD and Cryptography Techniques for Cloud Data Confidentiality and Integrity,” vol. 30, no. 6, pp. 31–45, 2019, doi: 10.3966/199115992019123006003.

[47] B. A. Jalil, T. M. Hasan, G. S. Mahmood, and H. Noman Abed, “A secure and efficient public auditing system of cloud storage based on BLS signature and automatic blocker protocol,” *Journal of King Saud University - Computer and Information Sciences*, Apr. 2021, doi: 10.1016/J.JKSUCI.2021.04.001.

[48] G. S. Mahmood, N. Hasan Hassoon, H. N. Abed, and B. A. Jalil, “International Journal of Computing and Digital Systems An Efficient and Secure Auditing System of Cloud Storage Based on BLS Signature.” [Online]. Available: http://journals.uob.edu.bh

[49] M. Shinde, A. Jaiswal, A. Shinde, M. Rushikesh, R. Nikam, and Maharashtra. Mumbai, "IRJET-Storage Security in Cloud Computing IRJET Journal Storage Security in Cloud Computing," *International Research Journal of Engineering and Technology*, vol. 134, 2008, [Online]. Available: www.irjet.net

fffffffff

ORIGINALITY REPORT

28%	13%	11%	21%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Institute of International Studies Student Paper	8%
2	Baidaa Abdulrahman Jalil, Taha Mohammed Hasan, Ghassan Sabeeh Mahmood, Hazim Noman Abed. "A secure and efficient public auditing system of cloud storage based on BLS signature and automatic blocker protocol", Journal of King Saud University - Computer and Information Sciences, 2022 Publication	4%
3	openaccess.altinbas.edu.tr Internet Source	2%
4	Submitted to NCC Education Student Paper	2%
5	journal.uob.edu.bh Internet Source	1%
6	Submitted to Sydney Institute of Technology and Commerce Student Paper	1%
7	Submitted to Info Myanmar College	

	Student Paper	1 %
8	Submitted to Cyryx College, Maldives Student Paper	1 %
9	prakashinfotech.com Internet Source	1 %
10	Submitted to CSU, San Jose State University Student Paper	1 %
11	Submitted to Jacksonville State University Student Paper	1 %
12	www.rishabhsoft.com Internet Source	<1 %
13	Submitted to Marist College Student Paper	<1 %
14	Submitted to TMC Institute in Tashkent Student Paper	<1 %
15	Submitted to Monash University Student Paper	<1 %
16	Submitted to University of Ghana Student Paper	<1 %
17	www.hindawi.com Internet Source	<1 %
18	Submitted to Kensington College of Business - Brunei	<1 %

	Student Paper	
19	ijcsit.com Internet Source	<1 %
20	Submitted to Kaplan University Student Paper	<1 %
21	Submitted to Royal Holloway and Bedford New College Student Paper	<1 %
22	S. Vinoth, Hari Leela Vemula, Bhadrappa Haralayya, Pradeep Mamgain, Mohammed Faez Hasan, Mohd Naved. "Application of cloud computing in banking and e-commerce and related security threats", Materials Today: Proceedings, 2021 Publication	<1 %
23	repo.ust.edu.sd:8080 Internet Source	<1 %
24	Submitted to Visvesvaraya Technological University, Belagavi Student Paper	<1 %
25	Submitted to University of Economics & Law Student Paper	<1 %
26	cuts-ccier.org Internet Source	<1 %
27	link.springer.com Internet Source	<1 %

28	www.csroc.org.tw Internet Source	<1%
29	Submitted to Kingston University Student Paper	<1%
30	journalofcloudcomputing.springeropen.com Internet Source	<1%
31	www.ijoser.org Internet Source	<1%
32	Communications in Computer and Information Science, 2014. Publication	<1%
33	Jian Shen, Jun Shen, Xiaofeng Chen, Xinyi Huang, Willy Susilo. "An Efficient Public Auditing Protocol With Novel Dynamic Structure for Cloud Data", IEEE Transactions on Information Forensics and Security, 2017 Publication	<1%
34	ijns.jalaxy.com.tw Internet Source	<1%
35	"Cloud Computing Solutions", Wiley, 2022 Publication	<1%
36	Submitted to Nanyang Technological University, Singapore Student Paper	<1%
37	Submitted to University of Bedfordshire Student Paper	<1%

38	etheses.bham.ac.uk Internet Source	<1 %
39	core.ac.uk Internet Source	<1 %
40	Submitted to King's Own Institute Student Paper	<1 %
41	Submitted to Mae Fah Luang University Student Paper	<1 %
42	Liu, Hongwei, Peng Zhang, and Jun Liu. "Public Data Integrity Verification for Secure Cloud Storage", Journal of Networks, 2013. Publication	<1 %
43	Submitted to Victoria University Student Paper	<1 %
44	www.isecure-journal.com Internet Source	<1 %
45	Submitted to Higher Education Commission Pakistan Student Paper	<1 %
46	www.jocm.us Internet Source	<1 %
47	www.rgnpublications.com Internet Source	<1 %
48	Chunbo Wang, Xiaoqiang Di. "Research on Integrity Check Method of Cloud Storage	<1 %

Multi-Copy Data Based on Multi-Agent", IEEE Access, 2020
Publication

49	Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom. "Cloud Computing Security: From Single to Multi-clouds", 2012 45th Hawaii International Conference on System Sciences, 2012 Publication	<1 %
50	Vikas Chouhan, Sateesh K. Peddoju. "Reliable verification of distributed encoded data fragments in the cloud", Journal of Ambient Intelligence and Humanized Computing, 2020 Publication	<1 %
51	collections.plymouth.ac.uk Internet Source	<1 %
52	downloads.hindawi.com Internet Source	<1 %
53	export.arxiv.org Internet Source	<1 %
54	ijesrt.com Internet Source	<1 %
55	ir.lib.uwo.ca Internet Source	<1 %
56	researchonline.federation.edu.au Internet Source	<1 %

57	www.ece.iit.edu Internet Source	<1%
58	"Cloud Computing and Security", Springer Science and Business Media LLC, 2016 Publication	<1%
59	"Frontiers in Cyber Security", Springer Science and Business Media LLC, 2020 Publication	<1%
60	"Multimedia Forensics and Security", Springer Science and Business Media LLC, 2017 Publication	<1%
61	Hui Tian, Fulin Nan, Chin-Chen Chang, Yongfeng Huang, Jing Lu, Yongqian Du. "Privacy-preserving public auditing for secure data storage in fog-to-cloud computing", Journal of Network and Computer Applications, 2019 Publication	<1%
62	Lecture Notes in Computer Science, 2016. Publication	<1%
63	Submitted to Limerick Institute of Technology Student Paper	<1%
64	Mehdi Sookhak, Mohammad Reza Jabbarpour, Nader Sohrabi Safa, F. Richard Yu. "Blockchain and smart contract for access control in healthcare: A survey, issues and	<1%

challenges, and open issues", Journal of Network and Computer Applications, 2020
Publication

65	Worku, Solomon Guadie, Chunxiang Xu, Jining Zhao, and Xiaohu He. "Secure and efficient privacy-preserving public auditing scheme for cloud storage", Computers & Electrical Engineering, 2013. Publication	<1 %
66	ceur-ws.org Internet Source	<1 %
67	doaj.org Internet Source	<1 %
68	ijarcsse.com Internet Source	<1 %
69	iris.unige.it Internet Source	<1 %
70	journals.plos.org Internet Source	<1 %
71	www.idexlab.com Internet Source	<1 %
72	Baidaa Abdulrahman Jalil, Taha Mohammed Hasan, Ghassan Sabeeh Mahmood, Hazim Noman Abed. "A secure and efficient public auditing system of cloud storage based on BLS signature and automatic blocker	<1 %

protocol", Journal of King Saud University - Computer and Information Sciences, 2021
Publication

---

73 Chunhua Li, Peng Wang, Changhong Sun, Ke Zhou, Ping Huang. "WiBPA: An Efficient Data Integrity Auditing Scheme without Bilinear Pairings", Computers, Materials & Continua, 2019
Publication

<1 %

---

74 Francesco Buccafurri, Vincenzo De Angelis, Gianluca Lax. "An integrity-preserving technique for range queries over data streams in two-tier sensor networks", Computer Networks, 2022
Publication

<1 %

---

75 Xiling Luo, Zequan Zhou, Lin Zhong, Jian Mao, Chaoyong Chen. "An Effective Integrity Verification Scheme of Cloud Data Based on BLS Signature", Security and Communication Networks, 2018
Publication

<1 %

---

76 Yongkai Fan, Xiaodong Lin, Gang Tan, Yuqing Zhang, Wei Dong, Jing Lei. "One secure data integrity verification scheme for cloud storage", Future Generation Computer Systems, 2019
Publication

<1 %

---

77 www.semanticscholar.org

Internet Source

<1%

Exclude quotes	On	Exclude matches	< 5 words
Exclude bibliography	On		

fffffffff

GRADEMARK REPORT

FINAL GRADE

/0

GENERAL COMMENTS

Instructor

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

PAGE 16

PAGE 17

PAGE 18

PAGE 19

PAGE 20

PAGE 21

PAGE 22

PAGE 23

PAGE 24

PAGE 25

PAGE 26

PAGE 27

PAGE 28

PAGE 29

PAGE 30

PAGE 31

PAGE 32

PAGE 33

PAGE 34

PAGE 35

PAGE 36

PAGE 37

PAGE 38

PAGE 39

PAGE 40

PAGE 41

PAGE 42

PAGE 43

PAGE 44

PAGE 45

PAGE 46

PAGE 47

PAGE 48

PAGE 49

PAGE 50

PAGE 51

PAGE 52

PAGE 53

PAGE 54

PAGE 55

PAGE 56

PAGE 57

PAGE 58

PAGE 59

PAGE 60

PAGE 61

PAGE 62

PAGE 63

PAGE 64

PAGE 65

PAGE 66

PAGE 67

PAGE 68

PAGE 69

PAGE 70

PAGE 71