IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 29, No. 1, February, 2024, pp. 261-268
Journal homepage: http://iieta.org/journals/isi

An Enhanced Cloud Storage Auditing Approach Using Boneh-Lynn-Shacham's Signature and Automatic Blocker Protocol

Teeb Hussein Hadi[1], Juliet Kadum[2], Qusay Kanaan Kadhim[2*], Shaymaa Taha Ahmed[2]

[1] Department of IT, Middle Technical University, Baghdad 10074, Iraq
[2] Department of Computer Science, University of Diyala, Baqubah 32001, Diyala, Iraq

Corresponding Author Email: dr.qusay.kanaan@uodiyala.edu.iq

https://doi.org/10.18280/isi.290126

Received: 14 August 2023
Revised: 27 November 2023
Accepted: 5 December 2023
Available online: 27 February 2024

Keywords:
public auditing, cloud computing, automatic blocker protocol, third-party auditors, cloud storage, Boneh-Lynn-Shacham's

ABSTRACT

Cloud computing technique enables consumers to benefit from online data storage services. Despite all the benefits of cloud computing, users cannot physically access external data, which makes protecting the privacy of data stored there much more crucial. In addition to allaying users' worries about not being able to confirm the accuracy of their cloud data, this will enable them to switch from local storage to the cloud. This made cloud customers reliant on Third-Party Auditors (TPA) to confirm the accuracy of cloud data because public cloud storage auditing is one of these crucial components. However, this audit process shouldn't introduce any security holes in the privacy of consumers' data or put them under undue Internet stress. There should be a capability to improve the TPA's dependability and safeguard the confidentiality of customer data stored in the cloud. This paper suggests a powerful public cloud data auditing users can confirm the authenticity of a signer using a cryptographic signature mechanism based on the Boneh-Lynn-Shacham (BLS) signature. To provide data privacy and public auditing, the system uses a bilinear pairing for verification. Signatures are components of an elliptic curve group. The suggested approach also implements batch audits and dynamic data processing.Additionally, the proposed system strengthens security authentication making use of the Automatic Blocker Protocol (ABP), a system-wide automatic blocker of any unauthorized unit. The system verifies the specific parameters, confirms the correct TPA protocol, and stops the unauthorized TPA when the client configures the parameters. The suggested approach is more effective, making it exceedingly safe and secure. The proposed method used the Berka data set, which compiles financial data from a Czech bank. Approximately 1,000,000 transactions involving over 5,300 bank clients are handled by the dataset. Furthermore, the dataset describes the almost 700 loans and nearly 900 credit cards that the bank represented in the dataset has extended and issued. As a result, the rate of cloud data auditing was 99% accuracy.

1. INTRODUCTION

A cloud computing paradigm is the next step in the evolution of an organization's Information Technology (IT), as it offers a number of unmatched services, such as self-service on demand, network access Quick resource adaptation, location independence, usage-based billing, and risk management are all possible from anywhere [1]. The usage of cloud computing by businesses will change how they use IT, and it is a positive experience. The data in this paradigm is targeted for use with cloud computing, which is one of its primary features [2]. According to users, including companies and people using information technology, there are many advantages to flexible on-request distant data storage in the cloud paradigm, including easing the burden of storage management, enabling global data access from various locations, and lowering costs for hardware, software, maintenance, etc. [3].

The cloud paradigm's foundational technology is cloud storage. Due to Its low price and good effectiveness, large-scale computing will develop from data centers service thanks to cloud data storage. Traditional storage systems are different from cloud storage. Large amounts of storage space and remote access to data are made available to consumers. To put it another way, any networked device linked to the cloud model can provide cloud users with simple access to external data, wherever they are, at any time [4].

Although the cloud model has many advantages, consumer's users of external data suffer security risks. As a result of the users' loss of control over their data, cloud service provider's controlling organizations vary. Consequently, there are numerous reasons why the accuracy of data in the cloud is at danger. First, dangers to data integrity from both the outside and inside affect cloud computing infrastructures; from time to time, notable cloud computing services have service outages and security breaches [5]. As a result, the public audit service is being activated for data saved using the cloud storage paradigm is essential because it enables cloud users to provide a third party permission to function as an unbiased auditor and analyze any necessary external data. This is a fast and simple approach so that users may check whether data stored in the cloud is accurate [6].

Along with cloud customers, the TPA project will assist cloud service providers by updating the cloud services platform [7]. Because users require a way to assess develop faith in the cloud and reduce dangers.

Cloud computing is described as "a model for enabling ubiquitous on-demand network access to a shared pool of configurable computing resources" (such as networks, servers, storage, applications, and services) that need little management work or service provider engagement and may be quickly provided and released " by the National Institute of Standards and Technology (NIST). This cloud modeling consists of three service models, four deployment modes, and five key characteristics [8].

There are many types of cloud computing, the Public Cloud On a pay-per-use basis, many enterprises can use a public cloud environment that is run by a third-party cloud service through the internet [9]. A quick and simple platform to deploy IT resources is what Small to medium-sized businesses with limited resources can benefit from public clouds [10].

Benefits of a public cloud include rapid scalability and no regional limitations. Efficiently priced the safest choice for sensitive data is not one that is highly reliable and simple to manage, and the Private Cloud a single company's modified infrastructure is used for this cloud distribution approach. It provides a precise setting where communication with IT resources is also concentrated within the company, the present instance may have shown either easily accessible managed internal. Even if private clouds are becoming more widely available, it might be able to alter the storing, interacting, and computing methods to satisfy all of their IT needs for significant productions [11].

The cloud storage both users of the cloud and providers of cloud services can gain from using a cloud storage solution [12]. Users of the infrastructure maintenance will no longer be a burden for the cloud because they incur the least expensive main investment costs. The user can access cloud services from any location by using cloud storage [13].

A range of methods, tools, and procedures are frequently used to protect cloud data. One key advantage of the cloud is the fact that many security components are already built into systems [14]. The challange of cloud computing technique enables consumers to benefit from online data storage services. Despite all the benefits of cloud computing, users cannot physically access external data, which makes protecting the privacy of data stored there much more crucial. In addition to allaying users' worries about not being able to confirm the accuracy of their cloud data, this will enable them to switch from local storage to the cloud. This made cloud customers reliant on Third-Party Auditors (TPA) to confirm the accuracy of cloud data because public cloud storage auditing is one of these crucial components. However, this audit process shouldn't introduce any security holes in the privacy of consumers' data or put them under undue Internet stress. There should be a capability to improve the TPA's dependability and safeguard the confidentiality of customer data stored in the cloud. Therefore, this study offers a reliable public cloud storage auditing system without requiring complete increasing the online workload for cloud users or recovering data, to verify cloud data and uphold privacy as needed. Additionally, it makes it possible for the TPA to manage several concurrent permission audits from a large number of prospective users in a safe and efficient way. Additionally, even when users add, delete, or modify data in the cloud, the suggested system allows using data dynamic operations, storage accuracy is guaranteed to remain at the same level [15]. By using security and performance evaluation, it is demonstrated that the suggested system is reliable and effective. For the purpose of offering public audits, privacy preservation, and batch auditing, the contribution proposes the BLS signature-based remote data integrity auditing system.

The suggested system also enables operations on dynamic data. The suggested system uses the Advanced Encryption Standard (AES) encryption method to enable information privacy in cloud storage environments. Increase a proposed scheme's the ABP's degree of security authentication to safeguard it against unapproved TPA. Analyze a suggested system's security and show that it is secure according to the random oracle paradigm [16].

2. RELATED WORKS

A number of secure deduplication algorithms have been proposed because Research and industry alike are interested in secure deduplication. Client-side deduplication attacks that can result in data leakage were demonstrated by Harnik et al. [17] introduces the idea of evidence of ownership to stop such assaults. Later, Bellare et al. [18] defined convergent encryption, which is known as message-locked encryption, and introduced a different technique, which is a server-aided encryption mechanism for deduplicated storage that ensures semantic security. Nevertheless, this audit protocol lacks capability for public data audit and has a limited audit number.Provable Data Possession (PDP) and Proof of Retrievability (POR) are two concepts that are developed to ensure data integrity in the cloud, created a verification system known as "provable data possession (PDP)" that is appropriate for cloud storage environments. Users only download a portion file to check the integrity of the protocol, which employs random sampling technology and an RSA-based homomorphic linear authenticator. The created a different "proof of retrievability (PoR)" approach that is appropriate for use in cloud storage environments. This scheme uses unique data blocks, often referred to as "sentinels," to implement data integrity detection in the data file, by Yu et al. [19] to ensure that cloud storage providers actually have the files without accessing or downloading the entire data. Between the verifier (a client or TPA) and the prover (a cloud), it essentially functions as a challenge-response protocol. In contrast to PDP, POR not only ensures that the target files are there on the cloud servers but also that they will fully recover. POR systems and PDP schemes have both been put forth since then.

Integrity auditing and security duplication cannot be effectively handled by a straightforward combination of public integrity auditing and secure duplication since attaining storage efficiency conflicts with the duplication of authentication tags. When a user uploads a file to a completely trusted TPA, they encrypt it using convergent encryption [20].

3. SYSTEMS MODELING

A three parts that make up the proposed public auditing model all have clear connections between them. The following main objectives need to be kept in mind while the system is first being designed:

Through public auditing, without needing to restore all data or imposing additional online responsibilities for cloud users, TPA can check cloud data upon request. Data privacy: for enable assurance of the suggested system's security. Protection of data integrity: To ensure that the proposed system's security and data integrity are safeguarded.

Privacy-preserving: to ensure the audit doesn't reveal any data content to the TPA. To allow the TPA to safely and efficiently handle several authorization audits from multiple potential users at once, batch auditing. Data dynamic support: for maintain a same level of storing accuracy guarantee regardless of user edits, deletions, or additions to data stored in the cloud. Figure 1 shows the suggested data auditing system.

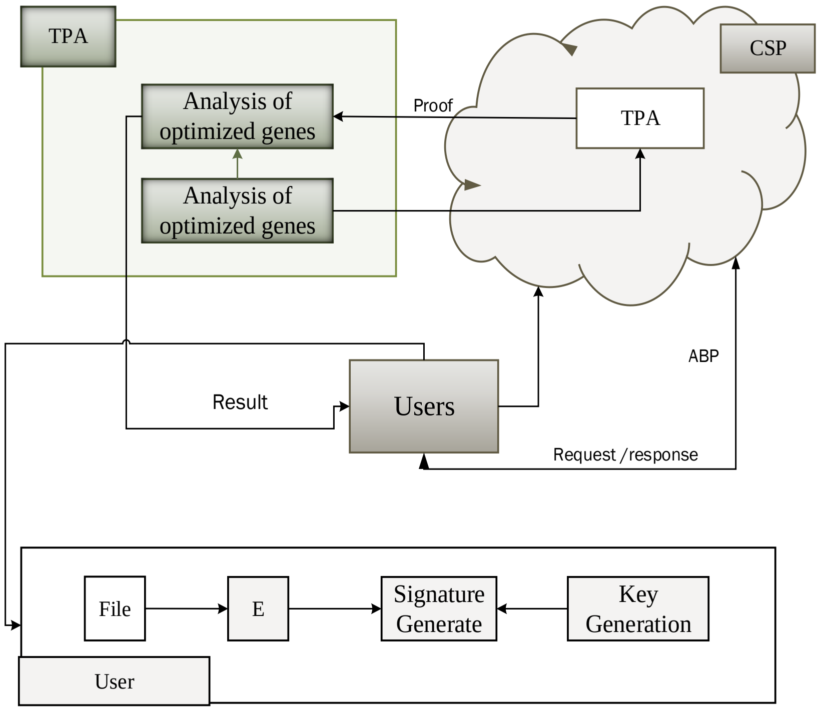

Figure 1. The proposed system

(1) Cloud server: It is a resource that is controlled Users can create, save, update, and request data retrieval using efficient tools provided from a cloud service provider (CSP). Additionally, it provides resources and expertise for outside house storage.

(2) User(s): Cloud users allocate IT-related work for experts and concentrate on one's own businesses while managing their data.

(3) Third-Party Auditor (TPA): Another organization with superior skills and knowledge that is utilized, when necessary, to evaluate the accuracy on behalf of users, dependability of cloud storage.

To cut down on storage and maintenance costs, large amounts of data can be kept by users on the cloud. The CSP is almost completely dependable, which means that it makes it possible for data to flow over the method consistently. Actual content data integrity, and reliability, however, might not be reliable, which means that a Cloud Service Provider might behave users are treated unethically in reference.

A mechanism for checking integrity must therefore be in place in order to correctly retain and protect user data. The responsibilities related to security audits can be delegated to TPA by the user [21].

3.1 Threat model

Consider a Cloud Service Provider that is essentially dependable and that is generally acting appropriately. But CSP might remove files that are hardly read. Or the Cloud Service Provider may choose to cover up data corruption to protect its reputation. Since the Third-Party Auditor is conducting an audit, we believe it to be trustworthy and independent, and as a result, there is no incentive for it to conspire with the Cloud Service Provider or the users during the audit. But if Third-Party Auditor can discover a data after auditing, it hurts the user.

As a result, two categories of dangers are linked to the accuracy of the information used by a cloud service provider. These threats are addressed below:

(1) Threat to Integrity: Data, the attacker can now see signatures as well as the public key. This attacker's objective aims to offer reliable evidence for data hacking.

(2) Threat to Privacy: Which the aggressor keeps track of evidence and information [22]. This attacker wants to learn further information, such as the nature or content of the data.

3.2 Boneh-Lynn-Shacham (BLS) signature

The Boneh-Lynn-Shacham signature system, first introduced in 2004, generates notably brief and secure signatures [23]. The BLS has some intriguing characteristics. These characteristics, which are depicted in Figure 2, will be covered in this section.

A group in which the decisional Diffie-Hellman (DH) issue can be solved effectively but the computational Diffie-Hellman (CDH) problem is unsolvable is known as a gap group. Such groups are allowed by non-degenerate, efficiently computable, bilinear pairings.

Given two prime order groups, G and GT, let e: $G \times G \rightarrow GT$ be a bilinear pairing that is efficiently computable and non-degenerate. Assume g is a generator of G. Take the CDH problem g, g^x, g^y as an example. It would seem that the pairing function e is not useful in calculating g^{xy}, the CDH problem's solution. It is hypothesized that this particular instance of the CDH problem is unsolvable. By evaluating whether $e(g^x, g^y)= e(g, g^z)$holds, we may determine whether $g^z = g^{xy}$ given g^z without having to know $x, y,$ or z. The bilinear characteristic $x+y+z$ times is used to show $e(g^x, g^y)= e(g, g)^{xy} = e(g, g)^z= e(g, g^z)$, then, since G_T is a prime order group, $xy=z$.

The ability to aggregate signatures is one of these attributes. We can calculate an aggregate public key P and an aggregate signature S that is validated with P given public keys $p_1, p_2..., p_n$ and associated signatures $s_1, s_2..., s_n$. It is possible to gradually add more signatures [9].

This means that with s_1 and s_2, we may generate the aggregate signature s_{12}. The total signature, s_{123}, can then be created by adding s_3. The technique is useful for many applications, including Public Key Infrastructure (PKI) and the secure protocol, because it condenses numerous signatures into a single, equal-length, compact signature [24].

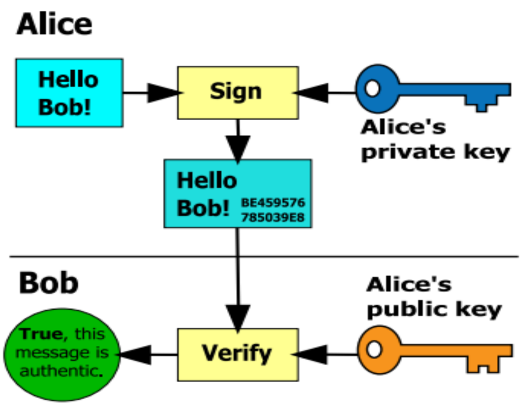

Figure 2. Boneh-Lynn-Shacham (BLS) signature [24]

Figure 2 An illustration of a public key signature technique [25]. Using her private key, Alice sings "Hello Bob!" and sends Bob the message along with its signature. The message's authenticity and integrity are confirmed by Bob using Alice's public key.

The unique and deterministic signatures generated by the BLS are useful. There can only be one legal signature for a specific set of public key and message. The use of randomization produces numerous potential valid signatures in other systems. The use of BLS results in deterministic operations across the board. It is crucial to reduce the computational overhead for many applications. BLS enables batch verification, which increases the effectiveness of signature verification.

The fundamental benefit of a BLS signature is the ability to combine several public keys into a single signature, allowing for the grouping of numerous signatures into separate messages. The three tasks performed by BLS are key creation, signature, and verification [26].

Three steps make up a signature scheme: produce, sign, and verify.

(1) Key generation

The key generation procedure selects an integer x, such as $0 < x < r$, at random. The secret key is x. The person who owns the private key discloses the public key, g^x.

(2) Signing

Using the bitstring m as a hash, we can calculate the signature given the private key x and the message m: $h = \mathrm{H}(m)$. The signature $\sigma = h_x$ is produced.

(3) Verification

Assuming a public key g_x and a signature σ, we confirm that $e(\sigma, g)=\mathrm{e}(\mathrm{H}(m),g_x)$.

3.3 Automatic Blocker-Protocol (ABP)

Any unapproved unit on the systems is automatically blocked by the ABP protocol. Upon the client having established the parameters, a system examines each specific parameter, confirms the correct Third-Party Auditor protocol, and blocks any unapproved TPA. If Third-Party Auditor the system triggers the security restrictions it had previously set up for the Third-Party Auditor configuration since it has lately gained access to the cloud server [27]. Present system achieves goal by exploiting technique Automatic Blocker Protocol (ABP). Present System show secure cloud storage architecture that allow an organization to store data securely in a public cloud, while maintaining the sensitive information related to the organization’s structure in a private cloud, enables a user to search encrypted data in the asymmetric encryption setting, associated with pixels for each of which a public key component is defined. The encrypted associates the set of attributes to the message by encrypting it with the corresponding public key components. Based on the proposed ABP scheme, the owner encrypts the data and features with public key encryption, which will be appropriately selected with regard to functionality and efficiency. To avoid the interaction with the owner for content access while still enforcing access control. The ABP ensures the information about the cloud user to the data owner.

3.4 Suggested system's methodology

A user must first sign into the system. Next, the cloud administrator will normally carry out the user registration procedure, during which the group user must register their details using personal information. The user receives a personal ID after completing the registration process to use while executing cloud dynamic data operations. If a user wants to update or modify their personal information, they must submit the appropriately changed information to the cloud administrator, who can then update and modify that pertinent user information. User divides data file into different data blocks after successfully login in, which are then encrypted using the Advanced Encryption System (AES) to ensure data confidentiality [27]. Thus, before uploading the data file to the cloud, the user receives the encoded version, E = $(e_1, e_2... e_n)$. Before transmitting a cloud model's encrypted blocks with for every encrypted block, the user first generates the private keys, public keys, and associated keys. Next, the user removes from local storage the data file and the corresponding signatures. The cloud user then assigns integrity auditing to the auditor when he needs to validate the data file. As a result, the auditor creates and sends a challenge to the cloud service provider. In order to improve authentication, the CSP sends a query to the user when it is confronted with a challenge by the auditor. A CSP agrees to take on the assignment and provides a supporting documentation back for the auditor if a user approves an investigation. The auditor can then return a user's results after verifying the data's validity, as shown in Figure 1.

Assume that G is the prime order pr 2 Zp and e multiplicative group. A bilinear map is indicated as G× G→GT, where g is G's generator. In addition, we enhanced the suggested system to enable batch auditing, which enables an auditor to review several files on several users' behalf. Additionally, the suggested system allows for dynamic data operations like additions, removals, and revisions.

4. RESULTS AND ANALYSIS

In this part, we assess the proposed system's performance using two metrics-a performance evaluation and security analysis utilizing the Berka Dataset.

4.1 Berka dataset

The Petr Berka and Marta Sochorova created the Berka Dataset. Financial data from a Czech bank are gathered in the Berka dataset. Over 5,400 bank clients and approximately 1,100,000 transactions are included in the dataset. Furthermore, the bank included in the dataset has issued nearly 900 credit cards and provided about 700 loans, all recorded in the data. Each account contains both static and dynamic features, such as payments debited or credited, balances given about "permanent order" and "transaction", and static characteristics, such as the date of creation and branch address, supplied regarding "account" and "account," respectively [3]. However, one benefit of Berka Dataset is that the training and testing datasets have a respectable amount of records. Because of this, running the trials on the complete collection is more economical than picking a random sample. The evaluation findings from many researchers will therefore be consistent and comparable.

4.2 Analysis of security

Security analysis, which is related to the suggested data auditing system and is reliant on the timing of deployment, is the most important factor. We must make sure that our plan satisfies the accuracy and soundness standards. Correctness refers to the response's ability to pass verification if the outsourced data on the data integrity are uncorrupted. Soundness indicates that verification can only be considered successful if the cloud outsourced data is intact.

4.2.1 Tokens' unpredictability

The file E's signature S for calculation, a proposed approach generates a random value (a). According to what was said earlier, this value is distinct for each block. The audit procedure was therefore impenetrable to the attacker. The cloud server can pass the requisite audit if it can fake the signature on the data [28]. However, to counterfeit the data signature, in order for the server to forecast the random value (a), it must be able to. Under a proposed system. Each modified new value will be added to block in the data file.

4.2.2 Guarantee of preserving privacy

This section shows that the proposed system has no information leaks, preventing the attacker from knowing anything about the audit process. An enemy like a malicious TPA and a challenger like a cloud server are the ones responsible for this process. We take the following actions to demonstrate this.

(1) The adversary chooses several name blocks (m_1,.....,m_k) for the challenge at random after receiving the user's information (Einfo=V_i,(m_i)), where V_i=gai).

(2) The blocks being challenged, the opponent issues an obstacle Q=i, q_i[1ik] and transmits Q to the contestant with a request for proof.

(3) Each block being tested, the challenger creates and gives the opponent the proof P=(S, p_k).

The suggested signature system uses an anti-collision hash function is called Hash (H). The attacker computes the hash function ((mi)) for the names of the challenged using blocks to check the accuracy of the cloud-stored blocks. After that, is used to confirm the accuracy of the data, which prevents the hostile adversary from accessing using the data via the signature (S), efficiently guaranteeing the secrecy of user data. However, all of the submitted parameters are checked by the system when a user configures the parameters, prevents After confirming the appropriate adversary protocol, the (ABP) is used to strengthen authentication against a system intrusion by an untrusted adversary, assuring a capability of the suggested system to secure user privacy.

4.2.3 Batch auditing provides security assurance

The complete signature is required for the batch verification process in the suggested method. Because of this, it is believed that the necessity to protect the confidentiality and privacy of numerous user files while batch verification is underway gives birth to the problem of single file security. Consequently, each user's file storage security and privacy preservation are guaranteed throughout the verification process. Likewise, it searches across many files. As a result, batch process verification is also given a security guarantee.

4.3 Evaluation of performance

An evaluation of the effectiveness of the proposed system is another crucial step that must be taken if we are to demonstrate the system's performance from all angles, including those of the user, auditor, and cloud service provider [29]. This section will evaluate the proposed system's efficiency in terms of communication and computin.

(1) Cost of computation: The expected compute cost of the system takes into account input from the cloud service provider, the third-party auditor, and the customer. To guarantee that the adoption of the suggested system is carefully assessed in order to achieve efficiency and protection through the use of the recommended methods.

(2) Cost of communication: The costs associated with communication stem from the processes of moving data to and from the cloud, as well as handling auditing issues. Since an independent auditor only requires several uploads and the cost is based on the chunks that the TPA has already provided for the inspection and the subsequent for its reaction, the suggested technique includes randomized chunks that the TPA chooses to dispute. The computing cost of the proposed system includes three sides: the user, TPA, and CSP. As a result, every aspect of the proposed system's implementation is scrutinized in order to ensure security and effectiveness of the suggested algorithms.

Figure 3 displays the segmented data with various data block numbers on the user side. As shown in Figure 3, the suggested system can separate the data of 100 blocks in less than 0.2 seconds. Data is divided into numerous blocks, and these blocks are then encrypted with the Advanced Encryption

Standard (AES) technique for preserve privacy. Figure 4 depicts the user-side computing expense encryption for various amounts of proposed system data contents. Figure 4 illustrates that the proposed method encrypts 500 KB of data in less than 0.20 seconds, compared to be 0.57 seconds. Because it provides greater data security for outsourcing and doesn't demand user resources while having reduced computational costs, the proposed system's crypto expense is still attractively cost. This ensures the proposed system's effectiveness.

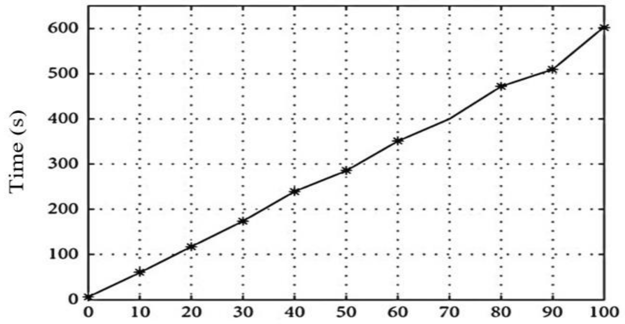

Figure 3. The cost of computing (The numbers of data blocks)

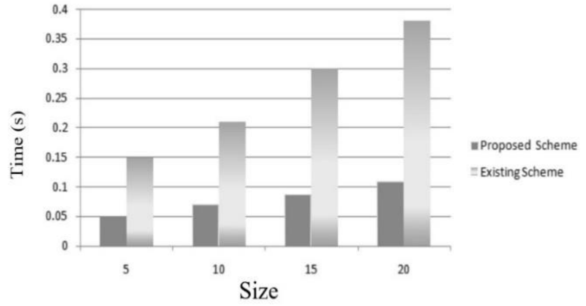

Figure 4. Cost of encryption calculation

After that, the keys and signatures are made by the user. Thus, it is evident that once (100) blocks have been chosen; key generation occurs quickly and takes just 0.014 seconds. However, the production of signatures takes more time each data block. Creating signatures to 100 block data files takes 0.067 seconds. When a file length is changed from 100 to 500 blocks and operation is timed, the suggested method, on the other hand, verifies the key creation and signatures. As projected to generate signatures for a particular file, with a roughly linear relationship to file size. More information about the keys and signatures created is provided in Figure 5.

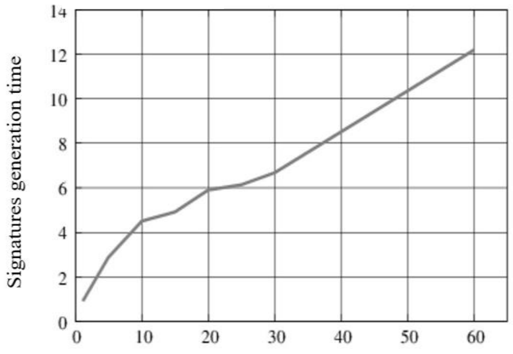

Figure 5. Generating signatures in time (Amount of data blocks)

However, from the perspective of the auditor, it creates a problem in addition to the auditing process. However, the proof generating procedure is exclusively done on the server-side. As it only takes 0.028 seconds to generate 100 KB, we can conclude that the challenge generation is quick. While checking proof and responding take more time. Then, we enhanced the quantity of work blocks from 100 to 500 in order to meet the time requirement.

As there are more challenges, it takes more time to create a challenge, an answer, and check evidence, as shown in Figure 6. Because of the suitability for experimental investigation, random values persist despite the increase in problematic blocks used to generate challenges must be trustworthy and since both the auditor and the cloud are performing more computations.

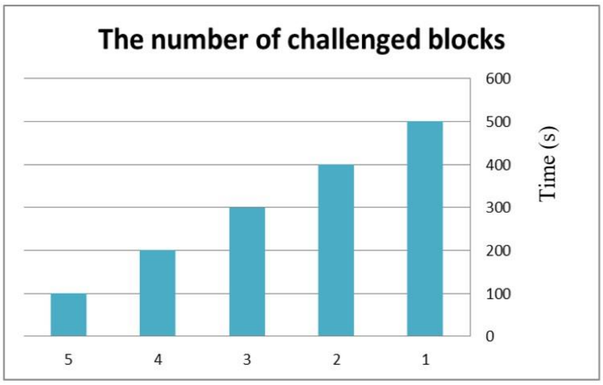

Figure 6. Times when evidence is generated

5. CONCLUSION

This paper discussed how to safeguard data confidentiality and precision in cloud computing. In our introduction to security concerns in cloud computing, we found that data security has grown to be a substantial obstacle. Numerous academics have investigated this issue and proposed solutions to confirm the legitimacy of cloud-based data. Most past studies have focused on static data sets. Batch auditing, dynamic data processing and the introduction of significant computing and communication costs are not supported. As a result, using a BLS signature-based public auditing mechanism, the cloud environment can store data anonymously. The data was encrypted using the AES encryption method before being sent to the cloud, achieving data privacy in cloud storage environments. This work proposes a robust public cloud data auditing system based on the Boneh-Lynn-Shacham (BLS) cryptographic signature technique, enabling users to authenticate signers. Bilinear pairing is used in the scheme to verify its integrity, and signatures—components of an elliptic curve group—ensure public auditing and data privacy. Dynamic data processing and batch audits are also implemented in the proposed method.

Furthermore, the suggested system uses the Automatic Blocker Protocol (ABP) to enhance security authentication. However, considering the persistence of the issue and the demonstrated security of the provided technique in a paradigm of random oracles, the TPA should go quickly and complete the verification. The suggested method explicitly shows that the processing price of evaluating data integrity for auditing is small because an authentication signature only contains one element. As a result, the cost of the signature's transmission and storage can be reduced. The method suggested is more successful, which makes it incredibly safe and secure; cloud data auditing had an accuracy rate of 99%. We plan to improve the functionality of our auditing approach in the future, including identifying and fixing faulty data blocks.

REFERENCES

[1] Youn, T., Chang, K., Rhee, K.H., Shin, SU. (2017). Public audit and secure deduplication in cloud storage using BLS signature. Information & Communication Technology Evolution (ReBICTE), 3(14): 1-10.

[2] Luc, N., Do, Q., Le, M. (2022). Implementation of Boneh - Lynn - Shacham short digital signature scheme using Weil bilinear pairing based on supersingular elliptic curves. Mathematics and Computer Science, 64(4): 3-9. https://doi.org/10.31276/VJSTE.64(4).03-09

[3] Jalil, B.A., Hasan, T.M., Mahmood, G.S., Abed, H.N. (2022). 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, 34(7): 4008-4021. https://doi.org/10.1016/j.jksuci.2021.04.001

[4] Nazeeh, I., Hadi, T.H., Mohammed, Z.Q., Ahmed, S.T., Kadhim, Q.K. (2023). Optimizing blockchain technology using a data sharing model. Indonesian Journal of Electrical Engineering and Computer Science, 29(1): 431-440. https://doi.org/10.11591/ijeecs.v29.i1.pp431-440

[5] Ahmed, S.T., Kadhem, S.M. (2021). Applying the MCMSI for online educational systems using the two-factor authentication. International Journal of Interactive Mobile Technologies, 15(13): 162-171. https://doi.org/10.3991/ijim.v15i13.23227

[6] Kadhim, Q.K., Yusof, R., Mahdi, H.S., Ali Al-Shami, S.S., Selamat, S.R. (2018). A review study on cloud computing issues. Journal of Physics: Conference Series, 1018(1): 012006. https://doi.org/10.1088/1742-6596/1018/1/012006

[7] Liu, S.G., Liu, R., Rao, S.Y. (2022). Secure and efficient two-party collaborative SM9 signature scheme suitable for smart home. Journal of King Saud University - Computer and Information Sciences, 34(7): 4022-4030. https://doi.org/10.1016/j.jksuci.2022.05.008

[8] Matoussi, W., Hamrouni, T. (2022). A new temporal locality-based workload prediction approach for SaaS services in a cloud environment. Journal of King Saud University - Computer and Information Sciences, 34(7): 3973-3987. https://doi.org/10.1016/j.jksuci.2021.04.008

[9] Kadhim, Q.K., Yusof, R., Selamat, S.R. (2018). The cloud computing control in the government services. Jour of Adv Research in Dynamical & Control Systems, 10(4): 1136-1147.

[10] Li, R., Yang, H., Wang, X.A., Yi, Z., Niu, K. (2022). Improved public auditing system of cloud storage based on BLS signature. Security and Communication Networks, 2022: 6800216. https://doi.org/10.1155/2022/6800216

[11] Yu, H., Cai, Y., Kong, S. (2016). An efficient public auditing scheme for cloud storage server. International Conference on Advanced Electronic Science and Technology (AEST 2016), pp. 725-730. https://doi.org/10.2991/aest-16.2016.97

[12] Ahmed, S.T., Khadhim, B.J., Kadhim, Q.K. (2021). Cloud services and cloud perspectives: A review. IOP Conference Series: Materials Science and Engineering, 1090: 012078. https://doi.org/10.1088/1757-899X/1090/1/012078

[13] Gupta, A., Siddiqui, S.T., Alam, S., Shuaib, M. (2019). Cloud computing security using blockchain. Journal of Emerging Technologies and Innovative Research (JETIR), 6(6): 791-794.

[14] Dhahi, S.H., Dhahi, E.H., Khadhim, B.J., Ahmed, S.T (2023). Using support vector machine regression to reduce cloud security risks in developing countries. Indonesian Journal of Electrical Engineering and Computer Science, 30(2): 1-8. https://doi.org/10.11591/ijeecs.v30.i2.pp1-1x

[15] Alsultani, H.S.M., Kanaan, Q., Khudhair, I.Y. (2018). Empirical investigation of TCP INCAST congestion in Wireless cloud computing networks. Journal of Computer Science, 14(5): 663-672. https://doi.org/10.3844/jcssp.2018.663.672

[16] Wang, S., Wang, X., Zhang, Y. (2019). A secure cloud storage framework with access control based on blockchain. IEEE Access, 7: 112713-112725. https://doi.org/10.1109/ACCESS.2019.2929205

[17] Harnik, D., Pinkas, B., Shulman-Peleg, A. (2010). Side channels in cloud services: Deduplication in cloud storage. IEEE Security & Privacy, 8(6): 40-47. https://doi.org/10.1109/MSP.2010.187

[18] Bellare, M., Keelveedhi, S., Diego, S., Ristenpart, T., Madison, W., Ristenpart, T. (2013). DupLESS: Server-aided encryption for deduplicated storage. 22nd USENIX Security Symposium (USENIX Security 13), pp. 179-194.

[19] Yu, Y., Au, M.H., Ateniese, G., Huang, X.Y., Susilo, W., Dai, Y.S., Min, G. (2017). Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage. IEEE Transactions on Information Forensics and Security, 767-778. https://doi.org/10.1109/TIFS.2016.2615853

[20] Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., Ishfaq, M. (2022). Blockchain technology: Benefits, challenges, applications, and integration of blockchain technology with cloud computing. Future Internet, 14(11): 341. https://doi.org/10.3390/fi14110341

[21] Almishal, A., Youssef, A.E. (2016). Cloud service providers: A comparative study. International Journal of Computer Applications & Information Technology, 5(2): 46-52.

[22] Ouda, G.K. (2020). Cloud computing service providers: A comparative study. Samarra Journal of Pure and Applied Science, 2(1): 76-89.

[23] Lacharité, M.S. (2018). Security of BLS and BGLS signatures in a multi-user setting. Cryptography and Communications, 10(1): 41-58. https://doi.org/10.1007/s12095-017-0253-6

[24] Ng, T.S., Tan, S.Y., Chin, J.J. (2018). A variant of BLS signature scheme with tight security reduction. International Conference on Mobile Networks and Management, 235: 150-160. https://doi.org/10.1007/978-3-319-90775-8_13

[25] Fan, H., Liu, Y., Zeng, Z. (2020). Decentralized privacy-preserving data aggregation scheme for smart grid based on blockchain. Sensors, 20(18): 5282. https://doi.org/10.3390/s20185282

[26] Liu, Q., Guo, R., Jiang, W., Ma, D. (2022). Parallel chain consensus algorithm optimization scheme based on Boneh-Lynn-Shacham aggregate signature technology. Journal of Computer Applications, 42(12): 3785–3791. https://doi.org/10.11772/j.issn.1001-9081.2021101711

[27] H Ahmed, F.Y., Yousif Ameen, S., Omar, N., Fattah Kak, S., Mikaeel Ahmed, D., Ameen, S.Y., Najat Rashid, Z., Maseeh Yasin, H., Mahmood Ibrahim, I., Abid Salih, A., M Salim, N.O., Mohammed Ahmed, A. (2021). A state of art for survey of combined iris and fingerprint recognition systems telemedicine investigation and recommendation for Duhok province view project a state of art for survey of combined iris and fingerprint recognition systems. Asian Journal of Research in Computer Science, 10(1): 18-33. https://doi.org/10.9734/AJRCOS/2021/v10i130232

[28] Khadhim, B.J., Kadhim, Q.K., Khudhair, W.M., Ghaidan, M.H. (2021). Virtualization in mobile cloud computing for augmented reality challenges. In 2021 2nd Information Technology to Enhance E-Learning and Other Application (IT-ELA), Baghdad, Iraq, pp. 113-118. https://doi.org/10.1109/IT-ELA52201.2021.9773680

[29] Kadhim, Q.K., Yusof, R., Mahdi, H.S., Selamat, S.R. (2017). The effectiveness of random early detection in data center transmission control protocol - based cloud computing networks. International Journal on Communications Antenna and Propagation (IRECAP), 7(5): 1-7. https://doi.org/10.15866/irecap.v7i5.10104