



International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: <https://www.svedbergopen.com/>



Research Paper

Open Access

Secure Certificate-Based Multi-Party Computation For Privacy Preservation in Cloud Data Security

M.B.C. Asha Vani¹, * S. Venkatesan², M. Ramakrishnan³

¹Research Scholar, Department of Computer Applications, Madurai Kamaraj University, Madurai, Tamil Nadu, India. (E-mail: ashavani.mbc@gmail.com).

²Research Scholar, Department of Computer Applications, Madurai Kamaraj University, Madurai, Tamil Nadu, India. (E-mail: svenkatesanres26@gmail.com).

³Professor and Head, Department of Computer Applications, Madurai Kamaraj University, Madurai, Tamil Nadu, India. (E-mail: ramkrishod@gmail.com).

Abstract— Cloud computing security and privacy maintenance have emerged as essential factors since cloud services rely more heavily now while exposing users to serious risks concerning sensitive information abuse and unauthorized access and data leakage incidents. Privacy protection measures in cloud systems need to be reliable because massive business and personal information demand protection which ensures confidentiality and builds user trust. Today's privacy-preserving solutions encounter three main problems that involve substantial computational demands as well as scale-oriented limitations and multiple privacy element control capabilities. The proposed paper presents Secure Certificate-based Multi-party Computation (SecuraMPC) as a novel privacy-preserving solution that enhances security performance no matter how challenging the situation becomes. Users can protect their data privacy throughout cloud systems through an efficient method which merges cryptography and multiple parties across distributed computing. SecuraMPC establishes an all-inclusive privacy solution which protects data confidentiality while maintaining integrity and access control and auditing operations during execution time. The SecuraMPC system follows several operational steps which secure processed sensitive data by limiting access to authorized users during its protected execution period. Secure computation models with certificate-based encryption ensure high privacy protection while maintaining acceptable processing speed in the proposed approach. The performance abilities of SecuraMPC exceed traditional techniques like PKI, IBE, AB, HE and SMC because it enables better data protection together with faster processing and minimal information loss. The actual implementation of SecuraMPC demonstrates its superiority over traditional privacy methods through diverse metrics from cloud-based tests that demonstrate advanced data security together with inspection capabilities.

Keywords - Cloud Computing, Data Security, Privacy Preservation, Certificate Authority, and Data Auditing.

1. INTRODUCTION

Cloud computing transformed the provisioning, sharing, and access of computational resources and data on the internet. Technology has enhanced in processing capacity, software development, and networking over time, propelling cloud computing to mature from an elite service to an ordinary solution for individuals and organizations [1]. The most critical aspect of cloud computing is that the management of hardware is shifted to distant data centers, with users having adaptable, on-demand, and cheap computing resources. The reason that this transition has occurred is because of the heightened availability of cheaper but more powerful processors, SaaS (Software as a Service) platforms becoming available, and highly efficient data center designs [2]. The fundamental concept behind cloud computing is to offer clients virtualized computing capacity via the internet without requiring them to deal with direct hardware administration and concentrate on the services they need, storage, computation, or specially required applications. This has enabled users to receive quality services like data storage, software, and computing capability without local infrastructures. Instead of using hardwires as storage for their data or host applications, cloud computing enables the user and firm to subscribe to such services whereby their data can be stored at remote data facilities, possibly abroad or even in a different continent. Amazon Elastic Compute Cloud (EC2) and Amazon Simple Storage Service (S3) dominate in this market segment, with unbounded storage capabilities and scalable compute power which one can upscale as much as he or she would like [3]. Both of them are extremely popular these days since they are both within budget and cost-effective as they do not force users to acquire costly hardware equipment. However, despite the extensive

benefits of cloud computing, the model presents certain challenges and threats that the consumers ought to understand. One of the primary fears is the availability and integrity problem of data. When consumers outsource their data to the cloud, they relinquish control of the physical media on which the data is being stored. The external providers, such as Amazon, Google, and Microsoft, are also liable for the hosting of the data in their data centers and their security and availability [4]. The external providers, although having strong infrastructures that consist of many data backups and security systems, introduce an element of vulnerability for the users due to their reliance on the providers. If there is a technical crash or shutdown, the users can lose access to their information and the consequences of this can be severe, especially for businesses that are making use of real-time access to information [5]. The comment highlighted the vulnerability of cloud computing, where business companies could not reach their vital applications and information, ranging from e-commerce websites to multimedia sharing services.

Amazon S3 failure demonstrated the disadvantage of letting data reside with a third-party cloud service provider, where it was beyond the customers' control due to a network problem in the provider infrastructure. Despite the enormous investment by cloud vendors in network operation, redundancy, and security, outages still happen. Although these outages are infrequent, they are symptomatic of the very reliance that end-users have on cloud service vendors for the reliability of data. Additionally, this paradigm [6] of outsourcing the management of data also poses issues about the privacy and security of the data. They must feel secure that cloud providers will put control measures in place to prevent others from accessing their data, to maintain it undamaged, and to protect it from hacking attacks. While cloud computing grows and develops, there should be recognition on both sides of the benefits of convenience balanced against control issues [7], weighing advantage from use of cloud facilities with disadvantage in accessibility to data, security risks, and loss of control.

From a data security point of view, Cloud Computing presents special and profound challenges which make it more challenging to maintain the integrity and confidentiality of data compared to traditional computing environments. This is largely because of the nature of cloud computing itself. In the classical models of computing, users are completely in control of their data, for instance, employing classic cryptographic methods to manage access and encrypt [7]. These methods cannot, however, be directly implemented in cloud environments because the user no longer owns the physical hard drives on which his data are stored. Cloud computing instead relies on the use of remote servers provided by third-party service providers, and users therefore only depend on such service providers regarding access and security to their data. Denial of direct access raises severe security and integrity issues of information within the cloud, particularly with regards to the volume of sensitive and critical information being hosted within such systems. Second, perhaps most urgently for security within cloud computing, is the assurance of data storage precision without users necessarily being aware of the full data set. In the conventional schemes, users have the ability to verify their data integrity by looking at it directly locally or via well-established primitives such as digital signatures or hashing. In the cloud, the users cannot physically see the data stored directly like in the earlier models [8], and hence new systems of data validation must be conceived that can securely and effectively work within the framework of the cloud model. The question of data storage validity is further compounded by the existence of users as they can be used to save various types of data ranging from documents and photos to complex databases, which are all capable of having different demands for security and storage. Also, ensuring long-term data integrity is required because cloud services retain data for a longer duration, thus one must have continuous verification processes that will ensure data will be intact and unchanged over a time span.

Unlike common static data storing systems, data in cloud computing is usually under continuous modification from users. Insertion, deletion, modification, appending, and reordering data are among operations included [9]. Operations are continuously run as users utilize their data and thus become a dynamic, regularly altering dataset. This dynamic nature of cloud data makes it difficult to guarantee data storage correctness. Common techniques of guaranteeing integrity, typically designed for static or less dynamic data sets, are in question in such scenarios [10, 11]. For instance, a simple hash of the data or cryptographic checksum may not suffice to offer data integrity in real time when data is being updated or modified continuously. Thus, new processes and methods must be established so that there can be great data integrity as far as the dynamic data nature in the cloud is concerned. These methods should be in a position to handle a sequence of operations changing the data yet make sure the data stored within the cloud does not change, is correct, and reliable.

Additionally, cloud deployment is primarily reliant on distributed centers of data executed simultaneously and parallelly over various geographical locations. Data centers replicate data redundantly across multiple physical locations for fault tolerance and reliability and high availability. Such redundancy reduces data loss resulting from equipment failure or region outages, but it results in complexity of ensuring data consistency. Cloud computing [12, 13] distributed architecture has the data not on a particular server or

site, and thus the usual means of ensuring data correctness cannot be used anymore. Thus, distributed protocols in new guise would need to provide correctness of data storage at multiple sites. These protocols have to be developed with the understanding of managing the intricacies of distributed systems, where the data is replicated on multiple servers and where synchronization and consistency between the replicas have to be ensured. Accuracy of data in this distributed setup needs to be guaranteed by advanced methods that are capable of solving issues such as network latencies, possible inconsistency of the data, and needing real-time updates on multiple servers.

The paper is organized in the following manner: Section 2 is a comprehensive literature review of existing security and privacy preserving models being used for cloud security, describing different methods and challenges of data protection in cloud environments. Section 3 illustrates the proposed model with an overview of its architecture, influential factors, and method of protection towards cloud security and privacy. Section 4 then introduces the performance and comparative result of the model proposed, with comparisons of its efficiency against other models based on the same measurements. Section 5 then concludes the paper's findings and contributions by summarizing potential directions of research and development of cloud security in the future.

2. Related Works

The past few years have seen rapid deployment of cloud computing, raising the serious issues of maintaining individuals and data private, and hence making it top cloud-based research topics [14]. With increasing people and organizations trusting their personal information to cloud service providers, preventing the information from falling into unauthorized hands, getting hacked, or even modified has been the biggest concern. Various models have been proposed to solve such concerns, like data protection during storage and transmission [15, 16]. Traditional techniques like encryption, access control, and secure authentication are typical but generally are insufficient to deal with specific needs in cloud infrastructures like multi-tenancy, fragmentation of information, and cloud resource dynamics. It is a more advanced set of methods that offer the confidentiality, integrity, and availability of users' information and are legal and regulative compliant. Various privacy-preserving models have been proposed, such as using homomorphic encryption, secure multi-party computation, and differential privacy [17]. The models aim at making secure access to sensitive information possible without releasing the data into the reach of potential attacks and therefore enabling legitimate cloud service providers to process and manipulate the data. While promising, in a majority of scenarios, such measures are challenging regarding issues of computational expense, scalability, as well as their implementability in cloud service infrastructure heterogeneity.

Cloud data security is an umbrella term utilized in the security control explanation that focuses on detection, prevention, and response to security threats. Another highly critical consideration to keep in mind is having cloud providers under close security control and end users controlling their data. They are responsible for creating an openness and audibility-centered model of security that will be powerful enough to make human beings more secure to use cloud computing. Wang, et al [18] introducing a new paradigm privacy-preserving time-based auditing for secure cloud storage with the aim to improve data integrity proofing without sacrificing user privacy. Here, the user can verify the integrity of uploaded files within a specific time frame without disclosing the user ID or file number to the Third Party Auditor (TPA). TPA verifies the integrity of the files but is only given the suspect time period so that no information of the user's individual files is disclosed. The method acts to address the increasing needs of data privacy by restricting the auditor to be given only the required time period and not the file content or figures. Beyond solving the deficits inherent in handling complex certificates in cloud storage systems, authors introduce an identity-based auditing system. This protocol minimizes overheads normally experienced in handling and authenticating certificates, making it a better-optimized and higher-efficiency solution for secure audits. The envisioned paradigm is a positive approach towards balancing cloud storage security and privacy, thus enabling users to authenticate their data integrity securely and maintain control over sensitive information.

Bingu, et al [19] provide a secure file management-based cloud auditing model with the guarantee of maintaining duplicate copies of encrypted files. The model is concerned with maintaining the integrity of every duplicate copy during public auditing and storage space conservation. One of the strongest features of the proposed technique is the offering of Secure Authentication with User Anonymity (SAUS), protecting the identity of the user and ensuring confidentiality throughout the copying and auditing process. To address the issue of having multiple auditing mechanisms for outsourced data, the paper proposes a model in which data integrity is maintained independently by each data owner and a delegating Third Party Auditor (TPA). This approach genuinely fixes the cloud storage problems by ensuring a safer, more robust, and more efficient auditing and management of data integrity for the cloud. Gautam, et al [20] suggest a new auditing model through lattice cryptography and an identity-based cryptosystem to counteract

quantum attacks and remove the necessity of certificates. With the inclusion of blockchain technology, the suggested framework improves the auditing process by monitoring the behavior of the cloud service provider and the Third Party Auditor (TPA). This unification lessens the dependency on TPA, necessitating a more open and decentralized process for auditing clouds. The security of the framework is carefully examined under the random oracle model with the Shortest Integer Solution (SIS) problem in lattices used to establish a quantum-resistant defense against possible quantum attacks. In terms of performance, the authors prove that the new mechanism is more computationally, communicatively, and storage-wise lighter compared to equivalent existing mechanisms and thus presents a more cost-effective solution to cloud security and auditing. Lattice-based cryptography makes it secure against future cryptattacks, and blockchain technology makes verifiable and secure auditability with fewer central authorities. It is an important improvement in cloud storage system security that preserves data confidentiality and integrity as well as safeguarding efficient performance of the system.

Liu, et al [21] develop a privacy-reserving dynamic auditing scheme for reparation code-based storage in an Industrial Internet of Things (IIoT) system assisted with cloud-fog. The introduced framework employs a generalized exact reparation regenerating code to encapsulate the data files, further securing data storage in this cloud-fog hybrid system. The encoding itself is done to secure data even under distributed storage scenarios, and for effective recovery of lost data in case of failures. Besides, authors also propose the use of the ZSS signature to sign each encoded piece of data as an authentication tag, thereby authenticating and ensuring data integrity. Another new data structure is also proposed to hold the encoded data and associated authenticators in the storage servers. The data structure makes maximum use of the fragmented storage, minimizing data update latency and improving the updating process. The solution resolves the security and performance issues of cloud-fog-assisted IIoT systems in such a way that it guarantees secure data storage as well as efficient management even in dynamic environments where data are under constant change. Ravikumara, et al [22] suggest a new security and access control strategy using biometric authentication in cloud systems. The biometric data is combined with other user information and securely transferred off the cloud provider in the method. The process operates by encrypting the request data using the biometric data provider beforehand before sending to the cloud. The cloud then executes a set of operations on the encrypted database, processes it, and sends the result to the data owner. This process is designed to provide security by making use of the biometric data for verification and ensuring that even though the attackers make an effort to access the data stored in the cloud, the encrypted data and security policies safeguard the user's sensitive data. A security review in the paper determines that the solution proposed provides protection at a high level, capable of safeguarding the data against unauthorized access even on attempted entry by hackers. The proposal is an accomplishment in the way biometric authentication is combined with cloud protection procedures, including user-friendliness as well as improved protection for users accessing stored information from the cloud.

While significant effort has been invested in cloud storage security and privacy-preserving protocols, there are several weaknesses and gaps in existing work. Current technologies are either designed for small-sized environments or they do not scale in large cloud environments [23] where large amounts of data are generated and stored in different locations. The issue is further aggravated by the issue of secure access control of data in multi-tenancy environments where data from multiple users should be separated and safeguarded from unauthorized users with maximum operations. The second key issue is the lack of an integrated approach with confidentiality, integrity, and availability of data in cloud computing. While most work focuses on a single or two aspects of security, in most scenarios, they are without end-to-end solutions that consider all three aspects of a comprehensive approach. In addition, most modern audit frameworks also utilize third-party auditors (TPAs) to a significant degree, and the result of this is introducing a point of trust that introduces the risk of violating users' privacy of data and greater overall reliance on centralized entities.

In addition, a majority of solutions for protecting privacy, particularly encryption and cryptography ones, are laden with extremely heavy computational and communications loads. They are responsible for degrading the performance, particularly in real-time systems where low latency is desirable as much as possible [24]. Though there are methods that utilize encryption to protect information, they appear not to focus on the possibility of light-weight and efficient means of encryption mechanisms with low processing or data accessing delay. This constraint is especially significant for distributed and dynamic cloud environments where data updates and real-time retrieval need to be guaranteed. Failing to prioritize quantum-resistant cryptography protocols is an overall constraint across existing research. As capability ramps up for implementing quantum computing, classical cryptographic algorithms will be subject to attack and cloud storage frameworks will be subject to new categories of attacks [25, 26]. But not many have developed quantum-resistant cryptography mechanisms or auditing methods, and future-proofing cloud security infrastructure is therefore an urgent necessity. Finally, though blockchain is a tempting

solution to more transparency and accountability of cloud systems, its application in cloud storage and audit systems is in its infancy. All the research papers emphasize the theoretical advantage of blockchain without maintaining the problem of practical implementation, i.e., energy wastage, low scalability, and congruence with the current cloud infrastructures. In summary, although highly relevant research papers have been presented on cloud security, they lack scalable, efficient, and quantum-resistant designs which can solve the complexity and dynamic threats present in contemporary cloud storage systems [27]. Loopholes faced in such works mean that more harmonious, dynamic, and intimate security steps will be taken, capable of meeting the rising need for cloud services.

3. Proposed Methodology

This work considers the increasing issue of data protection and privacy in cloud computing platforms, where sensitive data is offloaded and computed by third-party service providers. As more and more utilization of cloud services is increasing, maintaining data confidential and intact becomes more and more a point of concern, especially when computation is distributed among multiple parties. This approach enables the owners of the data to still have complete access to their private data while utilizing the computational strengths of cloud computer systems without opening up their personal data to strange third parties. The SecuraMPC model seeks to circumvent loopholes of usual security protocols of clouds by fashioning a safe protocol that features multiple parties involved, such as data owners, cloud computing servers, and free auditors. At the heart of the suggested approach is the use of Secure Multi-party Computation (SMC), through which computations are performed jointly by all the parties without any one party seeing other parties' raw, sensitive information. Certificate Authority (CA) also plays an important role in the suggested model, in that it provides digital certificates for all parties, guaranteeing authenticity, integrity, and non-repudiation of messages. The service provider computes the computation on encrypted data with homomorphic encryption technologies, keeping confidentiality of data in computation. The integrity and correctness of computations may be verified by third-party auditors without visibility into the actual data, with increased transparency and trust in the system.

The operation of the suggested SecuraMPC process is accomplished in a number of steps starting with the registration of parties such as the third-party auditor, the cloud service provider, and the data owners, and each is authenticated and verified by the Certificate Authority. After registration, the data owners encrypt their personal data with homomorphic encryption such that the data is secure when being computed. The cloud provider conducts calculations on the encrypted data itself without ever decrypting it and maintains the information confidential throughout. The third-party auditor also at regular intervals verifies the integrity of the data as well as of the calculations for ensuring that security and privacy policies are being implemented by the cloud service provider.

System Overview and Entities

SecuraMPC system is a complete system that is specifically designed to merge Secure Multi-party Computation (SMC) with a Certificate Authority (CA) to provide secure and privacy-preserving computing for cloud data security. It operates within the environment of a cloud computing infrastructure where multiple actors join forces in order to process the data so that confidentiality in the data under processing remains not compromised. The key stakeholders of the SecuraMPC model are the Cloud Service Provider (CSP), the Third-Party Auditor (TPA), and the Data Owners (DOs). The stakeholders within the system communicate to keep confidential data undisclosed as it is subjected to computations that are essential. The Certificate Authority is key in securing the system by handling and authenticating the identity of all parties. By using the public-key infrastructure (PKI), the CA guarantees the authenticity, integrity, and non-repudiation of the inter-party communications, thus creating a trust foundation that is essential to secure computation execution.

Data Owners (DOs) are such parties or entities who keep their sensitive data stored in the cloud and are concerned about its privacy and integrity. The Cloud Service Provider or CSP is the organization which keeps and processes the data securely within the cloud framework. Surprisingly, the CSP does this without ever having access to the underlying private data, thus ensuring the data confidentiality. Third-Party Auditor (TPA) is an independent third party that audits and verifies correctness of computations and ensures the cloud provider is conforming to privacy and security standards. The TPA is not given access to raw data but ensures integrity thereof and has an open auditability mechanism. The Certificate Authority (CA) manages and issues certificates to all the parties in the system, allowing one to trust and only allowing authorized entities to send messages to the system. The CA management of certificates guarantees that the identity of all parties is authenticated, making the whole framework secure and sound.

The system relies on a number of assumptions to ensure the parties' trust and security. One such assumption is that there exists a trusted Certificate Authority which is in charge of authenticating the identity of all parties involved in the system. This trust also accommodates the assumption that all Auditors

and Data Owners hold valid certificates issued by the CA, which allow them to communicate and function securely. Other than that, the CSP must keep data encrypted so that it does not see or read information stored in data that it has to process. The CSP may engage in secure computation over data in encrypted form without decrypting and keeping privacy. Finally, the TPA must be trusted so that it may check integrity in data without seeing data in raw form. This maintains the confidentiality of the data unaltered so that even though the TPA verifies correctness of calculations, the TPA will not be able to access confidential information, maintaining confidentiality of information throughout the process.

Secure communication and certificate management is facilitated by using Public Key Infrastructure (PKI), which allows one to validate and authenticate the parties. Homomorphic Encryption (HE) is a key method through which computations can be executed on encrypted information without decrypting. In other words, secret information can be kept confidential but processed securely in the cloud in a private manner. Secure Multi-party Computation (SMC) also expands the privacy of the system to such an extent that no party to the computation is able to view the private information of the other party. This allows several parties to collectively compute a function among their inputs without sharing the inputs with one another. Digital Signatures are used in an effort to ensure integrity and authenticity for each transaction or computation request submitted within the system. This ensures all computation is legitimate and traceable, and cannot be tampered with illegally. Finally, Zero-Knowledge Proofs (ZKPs) are employed to ensure that the cloud service provider functions correctly without ever receiving any private information. Employing these cryptographic protocols, the SecuraMPC model creates a very secure and privacy-protecting environment for data processing in the cloud. Fig 1 shows the overview of the proposed cloud data security and privacy preservation mechanism.

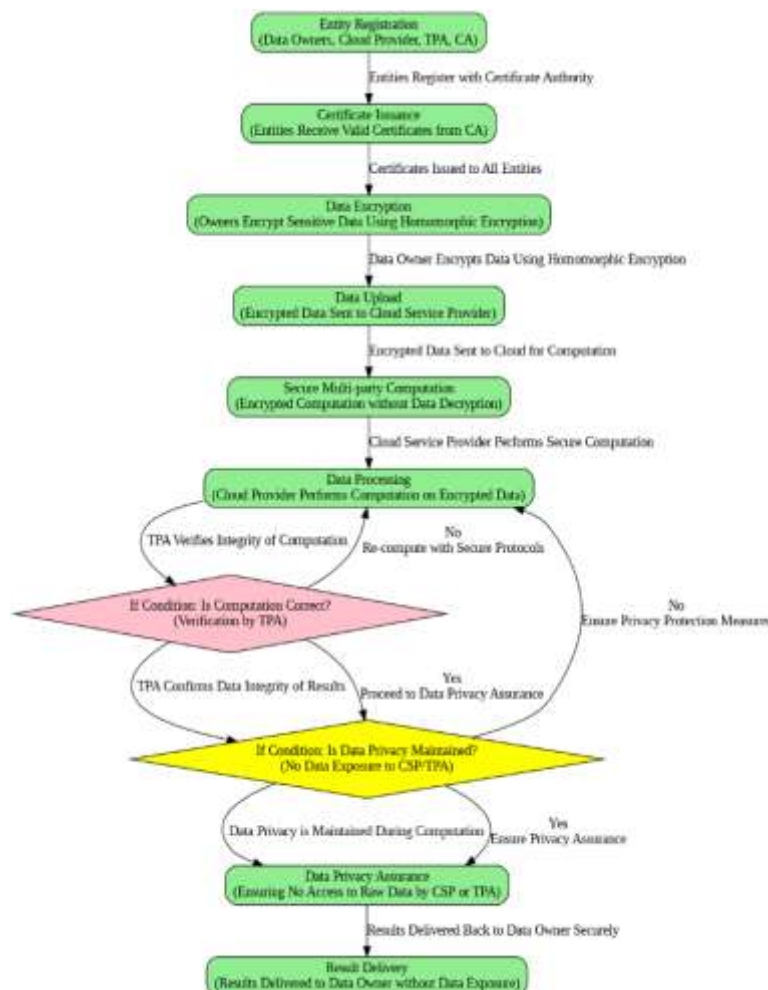


Figure 1. Overview of the proposed work

Secure Certificate-based Multi-party Computation for Privacy Preservation

The Secure Certificate-based Multi-party Computation for Privacy Preservation (SecuraMPC) protocol is a state-of-the-art privacy-preserving method that protects sensitive data in cloud storage scenarios. The protocol guarantees that owners of data are able to securely outsource computation to a cloud service provider (CSP) while retaining stringent privacy over their confidential information. The fundamental concept of SecuraMPC is to integrate Secure Multi-party Computation (SMC) principles and Certificate-based Authentication to ensure privacy and integrity while storing data as well as processing data. One of the main innovations and contributions of the method is that it can seamlessly merge cryptographic certificates with multi-party computation itself. With the help of a Certificate Authority (CA), the system ensures that only authorized and verified individuals or parties are permitted to be a part of the computation. The system is hence more secure and authentic in total, and nobody can hack the data or the process of computation without getting detected. The utilization of certificates for identity authentication, combined with homomorphic encryption and Secure Multi-party Computation protocols, renders the system highly secure even against advanced adversaries.

The conventional cloud computing models privilege centralized authentication schemes and trust models in that data owners must place their trust on the cloud provider for their data. SecuraMPC intervenes with a decentralized cryptographic certificate-based trust scheme in which the parties can conduct transactions securely and calculate without sharing any secret data. Homomorphic encryption guarantees that computations are being conducted on the encrypted data in a way that the cloud can compute the data without ever seeing the original, unencrypted data. This gives assurance that the data will remain confidential throughout the entire process from upload to computation and retrieval of the result. In addition, the system incorporates the third-party auditor (TPA), which monitors calculations being correctly carried out without any data privacy breach. SecuraMPC's primary contribution is to provide an efficient, secure, and privacy-preserving multi-party computation method for cloud infrastructure. With the addition of Secure Multi-party Computation and Certificate-based Authentication, the system also adds security to cloud data through the restriction of computation participation by trusted parties. This keeps the cloud service provider from being authorized with unauthorized access to sensitive information without offering instant and precise computations. SecuraMPC also provides an additional key contribution through the application of Zero-Knowledge Proofs (ZKPs) to enable the cloud provider to appropriately carry out computations. ZKPs enable the cloud to check with the data owner (or the auditor) that it has exactly carried out a computation, without ever revealing any of the intermediate information or data concerning the applied process.

This is particularly critical in uses where information is confidential and must be maintained so over its life cycle, even as it is being computed. Secondly, the Certificate Authority (CA) gives another layer of confidence and protection through the verification of all the stakeholders involved (cloud providers, data owners, and auditors) using a public-key infrastructure (PKI). This avoids depending on a conjectured central agency for trust and vulnerability to breaking into data due to illegal intrusions. The certificates are a guarantee of identity of the entities involved, and they guarantee high confidence of the message's authenticity and integrity. In the proposed SecuraMPC model, the homomorphic encryption is applied initially based on the following equation:

$$\mathcal{E}_h(m) = m^h \pmod{n} \quad (1)$$

Where, m indicates the encryption of original text, h is the encryption key, and n denotes the modules of encryption. Consequently, the encrypted values are added in the data as shown in below:

$$\mathcal{E}_h(m) \oplus \mathcal{E}_h(c) = \mathcal{E}_h(m + c) \quad (2)$$

Then, the encrypted values are multiplied for resulting in the encryption results using the following model:

$$\mathcal{E}_h(m) \odot \mathcal{E}_h(c) = \mathcal{E}_h(m \cdot c) \quad (3)$$

Similarly, the decryption is carried output for the encrypted data based on the following model:

$$\mathcal{D}_h(\mathcal{E}_h(m)) = m \quad (4)$$

Consequently, the multi-party computation process is performed based on the following equation:

$$\mathcal{S}_{MC}(m_1, m_2 \dots m_n) \rightarrow \text{Output}(\mathcal{F}(m_1, m_2 \dots m_n)) \quad (5)$$

Moreover, the certificate authority generates the public key as shown in below:

$$\mathcal{P}_{keyi} = CA(\mathbb{E}_i) \quad (6)$$

Where, $\mathcal{P}_{keyi}$ is the public key for each entity, CA is the certificate authority, and $\mathbb{E}_i$ is the entity. The digital signature is also generated for verifying the data integrity as shown in below:

$$\phi = \text{Sign}_{pri}(\rho) \quad (7)$$

Where, ρ is the message and ϕ indicates the generated digital signature. Then, the zero knowledge proof is also computed for verification as illustrated in below:

$$\text{Zero}_{KP}(m, \text{stmt}) \rightarrow \text{Valid} \quad (8)$$

Accordingly, the data privacy is ensured for secured communication in cloud.

Working Process

Data privacy and computational integrity stay protected during the entire SecuraMPC system operation which runs through a specified series of steps.

- The system commences after each stakeholder including data owners and cloud service providers and third-party auditors generates both an encryption key pair. The participants send their keys to a Certification Authority for verification of their respective identities. The Certificate Authority completes verification checks and provides digital certificates to each participant for verifying their identity and legitimizing their presence. The certificate serves as a fundamental foundation for authenticity since it stops illegal actors from accessing the calculation systems.
- The process of data encryption and upload begins after successful data owner authentication through the HE homomorphic encryption of their sensitive information. The data storage in the cloud provides resistance against cloud provider reading because of the encryption implementation. The cloud service provider receives encrypted data for processing after the owner completes the upload procedure. The data owner creates digital authentication through their private key which verifies both the stored information and preserves its integrity from storage to transmission.
- The cloud provider operates on encrypted data they receive through computation processes that do not involve decryption functions. Due to homomorphic encryption companies can execute mathematical operations on data which remains securely encrypted. The cloud functions without gaining knowledge about data contents throughout operations ensuring the protection of confidential information. The computation divide into segments that multiple entities including the cloud provider and data owner and possibly an auditor perform using Secure Multi-party Computation protocols during this stage. Parties use the system to do separate calculations for their data portions so that no single group receives complete access to sensitive information.
- Integrity Validation using ZKPs and Auditing: To check that indeed the computation has been performed correctly by the cloud provider, Zero-Knowledge Proofs (ZKPs) are employed by the third-party auditor (TPA). ZKPs enable the cloud to show to the auditor that it has performed the computation correctly without disclosing any sensitive intermediate values. The auditor will check the correctness of the computation and validate whether any tampering has taken place. This process compels the cloud provider to comply with the computation agreement terms and data secrecy.
- Once computation is finished and confirmed, the cloud sends the result back to the data owner. The result is decrypted using the secret key of the data owner, and the digital signature in the data guarantees the result is not tampered with or manipulated during transit.

4. Results and Discussion

Here, we discuss the assessment of the Secure Certificate-based Multi-party Computation (SecuraMPC) framework as suggested for providing privacy in cloud computing systems. SecuraMPC is designed to provide extended security by employing certificate-based authentication and multi-party computation (MPC) methods that collectively provide confidentiality, integrity, and authenticity of information

communicated in computation. The results in this paper evaluate SecuraMPC on a number of measures of privacy protection to demonstrate that it is as efficient as can be at offering robust privacy protection without adding undue overhead due to its privacy-protection measures. To effectively compare the performance of SecuraMPC, certain important parameters are examined: Privacy Protection Level, Processing Time, and Protection against Data Loss. These parameters give valuable indications about to what extent SecuraMPC achieves the tradeoff between privacy protection and computational cost and how it is in comparison with other known privacy preservation schemes like Secure Multi-party Computation (SMC), Homomorphic Encryption (HE), Attribute-based Encryption (ABE), and Public Key Infrastructure (PKI).

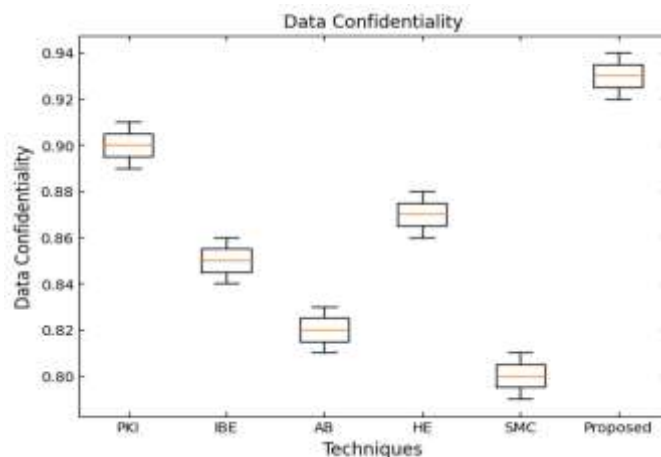


Figure 2. Comparison based on data confidentiality

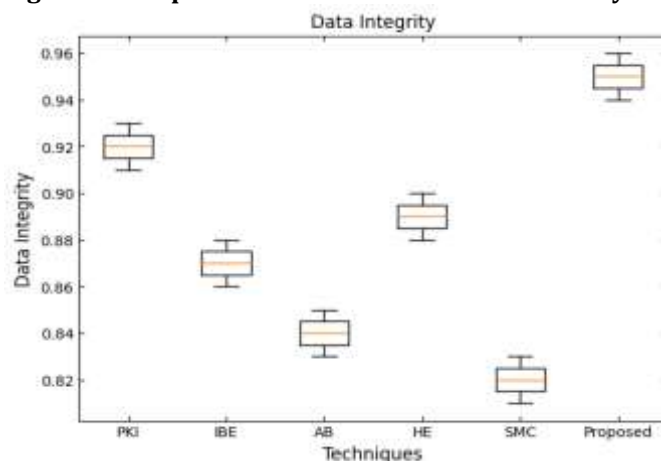


Figure 3. Comparison based on data integrity

Figure 2 compares the performance of different privacy preserving techniques for offering data confidentiality in different systems. Proposed technique offers better performance in confidentiality, leading others in all three evaluation phases. The high performance is due to the advanced encryption and multi-party computation methods implemented in SecuraMPC, which makes sure that only genuine parties have access to and can process confidential data. By comparison, PKI and HE are strong on confidentiality protection but short on performance compared to the solution described herein. Overall, Figure 3 demonstrates the supremacy of the proposed method in data protection from unauthorized access, with strong protection in dynamic cloud environments. Values in Fig 3 reflect that the proposed method is the best in ensuring data integrity, with values consistently greater than other methods. SecuraMPC provides better integrity because of its multi-layered cryptographic mechanisms, which recognize and prevent data tampering at every step of data handling. PKI and HE guarantee good data integrity but are relatively low in constant changing or interactive environments. SMC and ABE techniques provide moderate outcomes since their computational complexity causes some lag in authenticating real-time data that can potentially affect the overall integrity in vital operations. Fig 3 clearly illustrates that one needs to employ state-of-the-art privacy-saving technologies such as SecuraMPC in order to provide excellent data integrity without compromising performance.

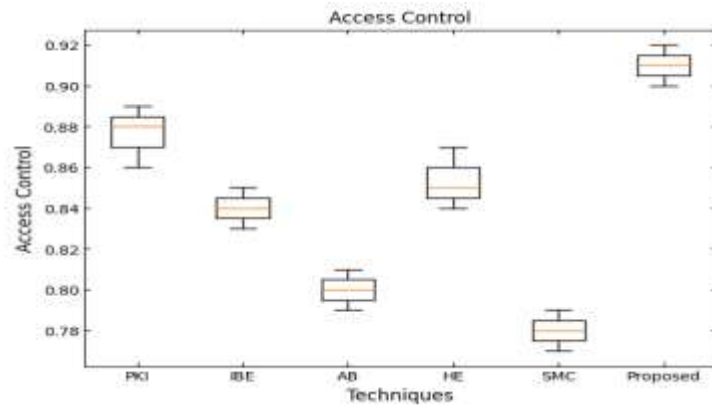


Figure 4. Comparison based on access control

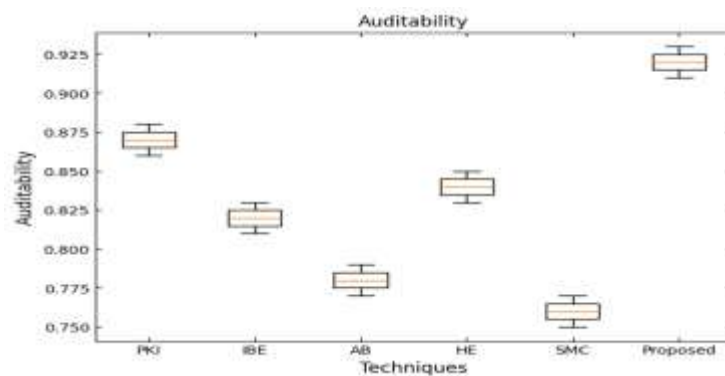


Figure 5. Comparison based on data auditability

In Figure 4, Proposed SecuraMPC demonstrates higher access control efficiency, where each comparison phase of the three comparison phases always achieves higher values. This is because it employs top-of-the-art authentication and access management protocols with dynamic updating access permissions to correspond to evolving security requirements. PKI and IBE provide sound access control but are rooted on static certificate-based systems, which are not optimal in highly changing cloud environments that have constantly altering access policies. SMC and HE grant some control of access but are not real-time responsive and thus less suited for sophisticated cloud infrastructures. Proposed methodology, in addition to maintaining strict control on data access, is more adaptive, thus greater scalability and responsiveness to shifting requirements of access. Fig 4 shows the role of dynamic mechanisms of access control in the protection of cloud systems with their growth in size and complexity. As shown in Figure 5, Proposed SecuraMPC performs better than other methods with increased auditability. This is due to the fact that it utilizes immutable audit trails, wherein data transactions and data changes are preserved in tamper-evident evidence. Techniques like PKI and SMC are auditability partial but cannot offer the detailed and up-to-date logs on distributed systems where data is always being updated or modified.

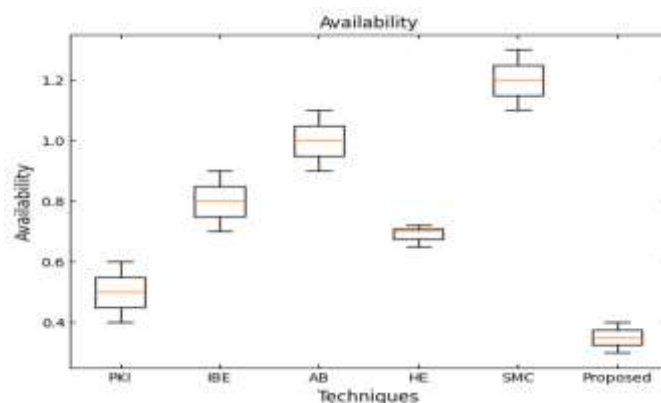


Figure 5. Comparison based on data availability

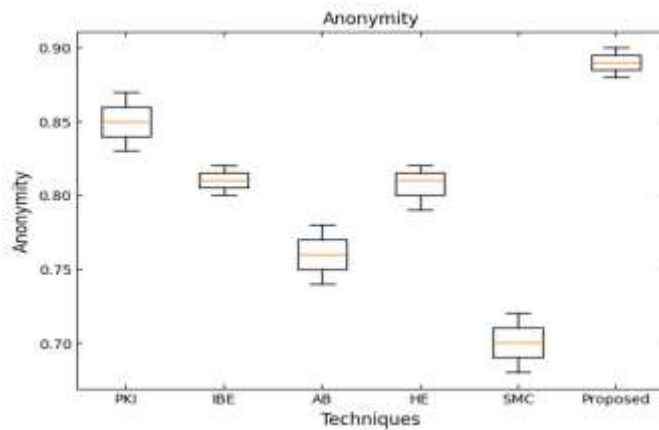


Figure 6. Comparison based on data anonymity

Figure 6 indicates that the proposed method is superior in delivering data anonymity, with the highest rates at each of the three levels of measurement. Methods like PKI and HE do offer some anonymity but are hampered by the use of conventional cryptographic techniques that are inadequate in situations calling for high anonymity. SMC and ABE offer moderate protection of anonymity but remain based on centralized management of data, which can violate anonymity in specific situations. The Proposed method, however, combines distributed privacy-preserving methods and is thus highly effective in providing data anonymity without compromising data utility. This picture depicts the increasing significance of cutting-edge privacy technology that enables users to have control over their own personal data while using cloud services.

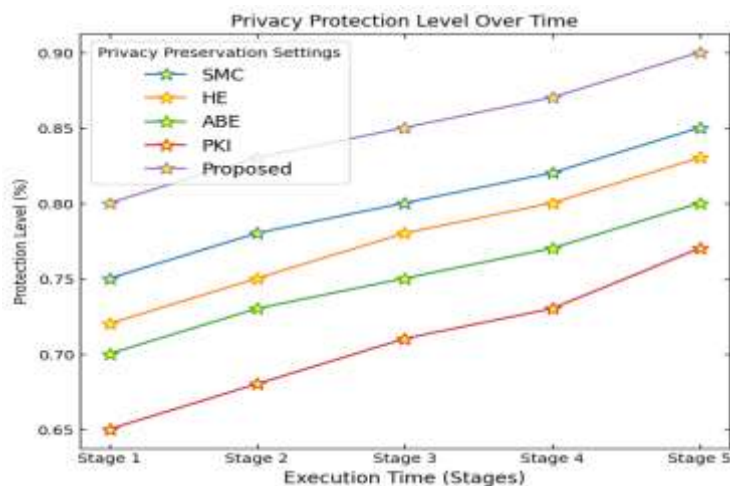


Fig 7. Privacy preservation level over time

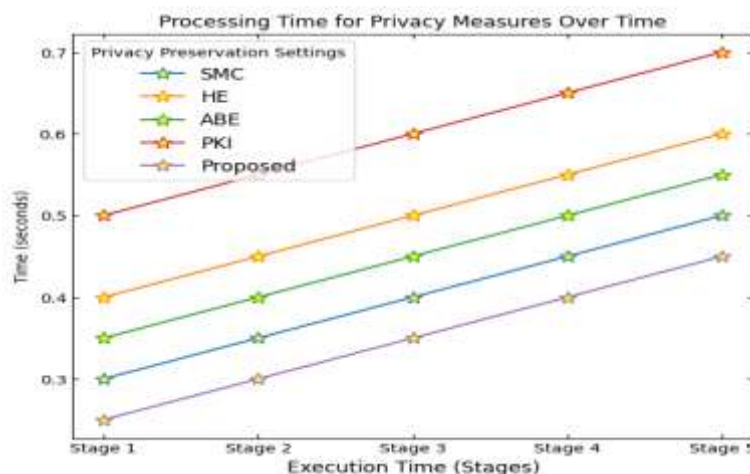


Fig 8. Processing time with respect to varying stages of execution

Fig 7 illustrates the privacy preserving level at each stage of execution of various privacy preserving approaches. The figure encloses the progress of each approach with consideration to how well it preserves data privacy as the process continues. From the figure, it is clear that the proposed method outperforms all other approaches at all five stages, with levels of privacy protection increasing gradually as the execution progresses. This means that SecuraMPC uses progressively advanced privacy-protecting mechanisms, thereby providing progressively stronger protection of sensitive data as it passes through consecutive rounds of computation. Unlike PKI, SMC, and HE techniques, they are comparatively steady but lower levels of privacy, which mean that their privacy-protecting ability does not grow with time or is conditional upon their intrinsic bounds. ABE continues to illustrate mediocre improvement yet without being able to match the progressive enhancement evident using the Proposed approach. The plot identifies the crucial advantage of the proposed solution: its adaptability and advancement ability in protecting privacy as computation advances, whereby robust confidentiality of information throughout the entire life cycle of processing is preserved. This renders the suggested solution extremely strong for situations where privacy requirements change over time, e.g., dynamic cloud systems or highly sensitive data systems.

Fig 8 plots the processing time taken by each method at each step of execution, namely in terms of the extra cost incurred by privacy. The story illustrates a severe trade-off between processing time and preserving privacy, where increasing processing time is typical of most of the techniques as they pass through each subsequent phase. The PKI and SMC techniques exhibit progressively rising processing times, mainly because of the high cryptographic and computationally intensive demands of their security measures. Despite achieving privacy protection effectively, the techniques are weighed down by delays that are risky in use cases that have sensitive timing concerns. In contrast, proposed method has the shortest processing time with the minimal growth in time when stages pass by. Proposed methodology probably takes more effective algorithms into use that keep security and performance in line without causing considerable lag. An increase in the time of processing is still realized step by step, but the pace is appreciably low when compared with other processes. This proves that the proposed approach can successfully reduce the overhead usually incurred by using privacy-protecting mechanisms and, hence, is more appropriate for real-time or voluminous systems. HE and ABE share moderate processing time increases, and they provide privacy protection but at some cost of system efficiency. In general, Fig 8 focuses on the suggested solution's enhanced efficiency, which is of extreme importance in retaining levels of performance in order to guarantee high protection levels of privacy through different phases of implementation.

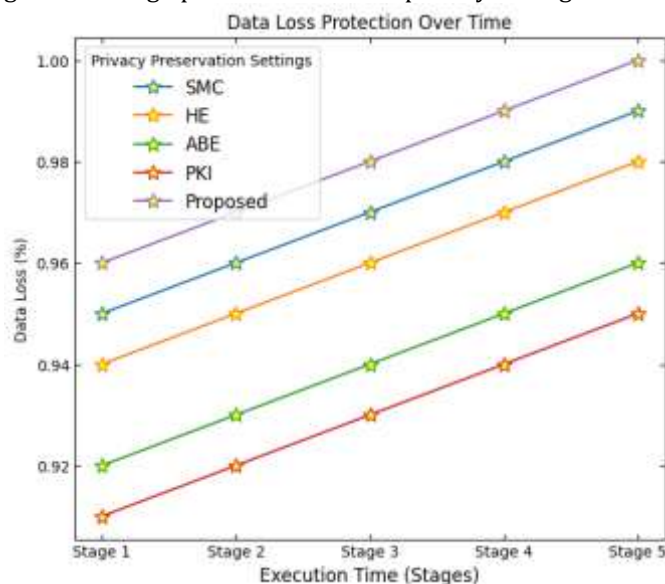


Fig 9. Data loss with respect to varying stages of execution

Fig 9 illustrates how good each technique is in data loss protection at each stage of execution. The Proposed technique illustrates the best data loss protection with values closest to perfect (0.96-1.0) at all stages, indicating it always provides minimum data loss at each stage of the process. This high data protection is a must in cloud environments where even slight data loss can be disastrous. The resistance of the proposed method comes from its advanced privacy-protection algorithms in which data integrity and loss prevention take priority in secure multi-party computation and encryption methods. This is compared to techniques such as PKI and SMC, in which there is less data security slightly below optimal followed by a weak decline in performance when the process progresses, a direct result of vulnerability to data loss when handling

very complex or large tasks. HE and ABE also follow the same pattern, providing effective protection against data loss but lagging behind the proposed method in subsequent phases. These methods are less efficient in evading data loss, perhaps because their cryptographic or encryption systems are weak. The graph merely substantiates the fact that although all the methods provide some form of data protection, the Proposed method is superior when it comes to reducing data loss and data integrity while processing and hence can be a highly dependable solution for critical applications where data protection is a must.

CONCLUSION

This paper presents a novel privacy protection mechanism for cloud computing systems using the Secure Certificate-based Multi-party Computation (SecuraMPC) approach. Employing the latest cryptographic methods and secure multi-party computation, the solution guarantees strong privacy preservation while system performance is guaranteed. By comparing with other privacy technologies in the market such as PKI, IBE, AB, HE, and SMC, the experiment result validates that SecuraMPC is better than all these systems in various ways such as privacy protection, integrity, access control, and data loss, at various levels of implementation. Performance analysis identifies flexibility in the case of SecuraMPC to combine evolving needs of preserving privacy without sacrificing either performance loss or system overhead. The approach outlined is seen to achieve improved security against data loss particularly in usage cases where data confidentiality and integrity are top priorities. The ability of the approach to provide high privacy with optimized processing time and maximum data retention is a valuable contribution to cloud security research. Further optimizations and application of SecuraMPC together with other upcoming future privacy-safeguarding technology can be performed by subsequent work to tackle the dynamic and complexity of current cloud systems. The demonstrated results show that SecuraMPC works as a secure solution that enables both scalability and performance enhancement for privacy protection in cloud environments.

REFERENCES

- [1] J. Yu and W. Shen, "Secure cloud storage auditing with deduplication and efficient data transfer," *Cluster Computing*, vol. 27, pp. 2203-2215, 2024.
- [2] H. Ali, S. Abidin, and M. Alam, "Auditing of Outsourced Data in Cloud Computing: An Overview," in *2024 11th International Conference on Computing for Sustainable Global Development (INDIACom)*, 2024, pp. 111-117.
- [3] S. Zeng, C. Hsu, L. Harn, Y. Liu, and Y. Liu, "Efficient and Privacy-Preserving Skyline Queries over Encrypted Data under a Blockchain-Based Audit Architecture," *IEEE Transactions on Knowledge and Data Engineering*, 2024.
- [4] J. Yu, W. Shen, and X. Zhang, "Cloud storage auditing and data sharing with data deduplication and private information protection for cloud-based EMR," *Computers & Security*, p. 103932, 2024.
- [5] R. P. Kumar and S. R. Bandanadam, "Block chain-based decentralized public auditing for cloud storage with improved EIGAMAL encryption model," *International Journal of Information Technology*, vol. 16, pp. 697-711, 2024.
- [6] F. J. Ekaputra, A. Ekelhart, R. Mayer, T. Miksa, T. Šarčević, S. Tsepelakis, et al., "Semantic-enabled architecture for auditable privacy-preserving data analysis," *Semantic Web*, vol. 15, pp. 675-708, 2024.
- [7] K. Gokulkannan, M. Parthiban, S. Jayanthi, and M. Kumar, "Cost effective cloud-based data storage scheme with enhanced privacy preserving principles," *The Scientific Temper*, vol. 15, pp. 2104-2115, 2024.
- [8] D. Kumari, P. Kumar, and S. Prajapat, "A blockchain assisted public auditing scheme for cloud-based digital twin healthcare services," *Cluster Computing*, vol. 27, pp. 2593-2609, 2024.
- [9] M. Chawki, "An effective cloud computing model enhancing privacy in cloud computing," *Information Security Journal: A Global Perspective*, pp. 1-24, 2024.
- [10] O. Zarichuk, "Security in cloud computing: Methods for ensuring privacy and integration in modern applications," *Development Management*, vol. 1, pp. 37-45, 2024.
- [11] S. R. Bashir, S. Raza, and V. Mistic, "Progress in Privacy Protection: A Review of Privacy Preserving Techniques in Recommender Systems, Edge Computing, and Cloud Computing," *arXiv preprint arXiv:2401.11305*, 2024.
- [12] L. Wang, M. Hu, Z. Jia, Z. Guan, and Z. Chen, "SStore: an efficient and secure provable data auditing platform for cloud," *IEEE Transactions on Information Forensics and Security*, 2024.
- [13] G. Kambala, "Data Privacy in Cloud Computing: A Comparative Study of Privacy Preserving Techniques," *International Journal of Scientific Research and Management (IJSRM)*, vol. 12, 2025.

- [14] M. Pavithra, M. Prakash, and V. Vennila, "BGNBA-OCO based privacy preserving attribute based access control with data duplication for secure storage in cloud," *Journal of Cloud Computing*, vol. 13, p. 8, 2024.
- [15] S. Yang and J. Chang, "Identity-based remote data integrity auditing from lattices for secure cloud storage," *Cluster Computing*, pp. 1-12, 2024.
- [16] K. Sundar, G. K. Vishwak, and S. G. Eswaran, "Enhancing Cloud Security: Secure and Auditable Data Sharing and its Implementation," in *2024 2nd International Conference on Networking and Communications (ICNWC)*, 2024, pp. 1-6.
- [17] J. Chen, T. Zhou, S. Ji, H. Tan, and W. Zheng, "Efficient public auditing scheme for non-administrator group with secure user revocation," *Journal of Information Security and Applications*, vol. 80, p. 103676, 2024.
- [18] M. Wang, J. Yu, W. Shen, and R. Hao, "Privacy-Preserving Time-Based Auditing for Secure Cloud Storage," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 7866-7878, 2024.
- [19] R. Bingu and S. Jothilakshmi, "Cloud auditing and authentication scheme for establishing privacy preservation," *Multimedia Tools and Applications*, vol. 83, pp. 43849-43870, 2024.
- [20] D. Gautam, S. Prajapat, P. Kumar, A. K. Das, K. Cengiz, and W. Susilo, "Blockchain-assisted post-quantum privacy-preserving public auditing scheme to secure multimedia data in cloud storage," *Cluster Computing*, vol. 27, pp. 8159-8172, 2024/09/01 2024.
- [21] D. Liu, Y. Ding, G. Yu, Z. Zhong, and Y. Song, "Privacy-preserving dynamic auditing for regenerating code-based storage in cloud-fog-assisted IIoT," *Internet of Things*, vol. 25, p. 101084, 2024.
- [22] R. Ravikumara and N. Thillaiarasu, "Privacy preserving biometric system based secure data access and public auditing method in cloud computing," in *AIP Conference Proceedings*, 2024.
- [23] S. Venkatesan and M. Ramakrishnan, "A Smart Coherent Security Model (SCSM) using Intelligent Optimization and Ensemble Deep Learning Mechanisms for Healthcare-IoT Networks," in *2024 Control Instrumentation System Conference (CISCON)*, 2024, pp. 1-9.
- [24] Y. Yuan, F. Yang, X. Wang, Y. Tian, and Z. Li, "Multi-replicas integrity checking scheme with supporting probability audit for cloud-based IoT," *PeerJ Computer Science*, vol. 10, p. e1790, 2024.
- [25] S. Velugoti and M. Vani, "An Approach for Privacy Preservation Assisted Secure Cloud Computation," *Informatica*, vol. 47, 2024.
- [26] S. Venkatesan and M. Ramakrishnan, "Energy Efficient of IDS Using Fuzzy Logic for Lifetime Improvement in Wireless Sensor Network."
- [27] S. Venkatesan, M. Ramakrishnan, and M. Archana, "An Innovative SALO-IDT-Based Intrusion Detection Model for Increasing the Security of IoT Networks," in *National Conference on Control Instrumentation System Conference*, 2018, pp. 313-327.