International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

An Effective Double Verification-Based Method for Certifying Information Safety in Cloud Computing

M. Amanullah[1], Ved Prakash Mishra[2], L Mayavan[3], Hendy Tannady[4], Nandini Kulkarni[5], Raenu Kolandaisamy[6]

Submitted: 25/04/2023 **Revised**: 12/06/2023 **Accepted**: 24/06/2023

Abstract: Cloud computing is an architectural concept that offers computation and storage space as a service as well as on-demand, dynamic access to any type of service over the Internet. Storage as a service is one of the major services offered. Data are stored and managed at a cloud provider's data centre using cloud computing services, which are entirely internet-based technology. Traditional cryptographic security based on the assumed difficulty of computer operations is facing tremendous challenges as a result of the evolution of information technology. The key concerns with cloud servers are successful safe communication and protecting sensitive data from unauthorized access on public networks. This protocol can be implemented using the exclusive-OR operation in traditional cryptography. Data security issues and supporting data security architecture are the key targets of this investigation. In the same way that it chooses a server for data storage that is quick, efficient, and light on resources, the system is made to prepare security procedures regardless of the order in which the data is stored. Cuckoo Search Algorithm (CSA) has been used to determine which available server is most suitable for a given task in wake-sleep distributed computing. Homomorphic encryption, where information is encrypted before being delivered to the server, is typically used to guarantee the veracity of the data being transmitted. To save on server resources and data storage, we've encrypted everything with ECDSA on the cloud server. It strengthens protections for user data in the cloud. At the end of the day, the system proves that data is secure, reliable, and private. Despite some drawbacks, this framework does provide safe methods of exchanging keys and backing up data, both of which are crucial for protecting the confidentiality of sensitive data kept in the cloud.

***Keywords*:** *Cloud computing, Cryptographic security, ECDSA, CSA.*

1. Introduction

Over the past ten years, cloud computing has become a potent computing platform with several benefits for both clients and providers. One of the most obvious and significant benefits is that clients can outsource their difficult computations and pay little or nothing for the latest technology and computing resources. One of the key justifications for the widespread use of cloud computing in various industries is the advantages offered by cloud technologies when contrasted with the expenses [1]. Although many businesses have demonstrated their preparedness to use the cloud and take advantage of its capabilities over the past several years, businesses are increasingly realizing that there are numerous security concerns that must be addressed when moving operations to the cloud [2].

A new paradigm known as "cloud computing" has recently arisen for providing customers with a variety of services, including servers, storage, software development platforms, and other platforms over the internet. Also, cloud computing offers both consumers and businesses a variety of options for their effective and efficient use of cloud services without raising the cost of computing resources [3]. A company can implement a private, public, or hybrid cloud, depending on its particular demands and security concerns. The majority of businesses are implementing this rapidly expanding paradigm to suit their computing needs and advance their operations [4]. With the help of a cloud service provider, consumers and businesses can use resources like network capacity,

1Professor, Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai 602117, India.
amanhaniya12@gmail.com
0000-0002-5423-9469
2Associate Professor, Computer Science and Engineering Amity University Dubai, UAE
mishra.ved@gmail.com
orchid id: 0000-0003-1832-8736
3Associate Professor Department of English Panimalar Engineering College, Chennai, India
mayavan1503@gmail.com
4Department of Management
Universitas Multimedia Nusantara,Banten, Indonesia
hendy.tannady@umn.ac.id
https://orcid.org/0000-0001-6911-7010
5Deputy director,Symbiosis School of Planning Architecture and Design Nagpur. Symbiosis International University, Nagpur. India.
deputydirector@sspad.edu.in
orchid id : 0000-0001-9575-9113
6Institute of Computer Science and Digital Innovation, UCSI University, Kuala Lumpur, Malaysia
raenu@ucsiuniversity.edu.my
https://orcid.org/0000-0003-0556-7770

storage, server utility, and other applications for a variety of services. This enables consumers to employ cloud platforms as a service, infrastructure as a service, and software as a service rather than investing in new hardware or software for their commercial needs [5].

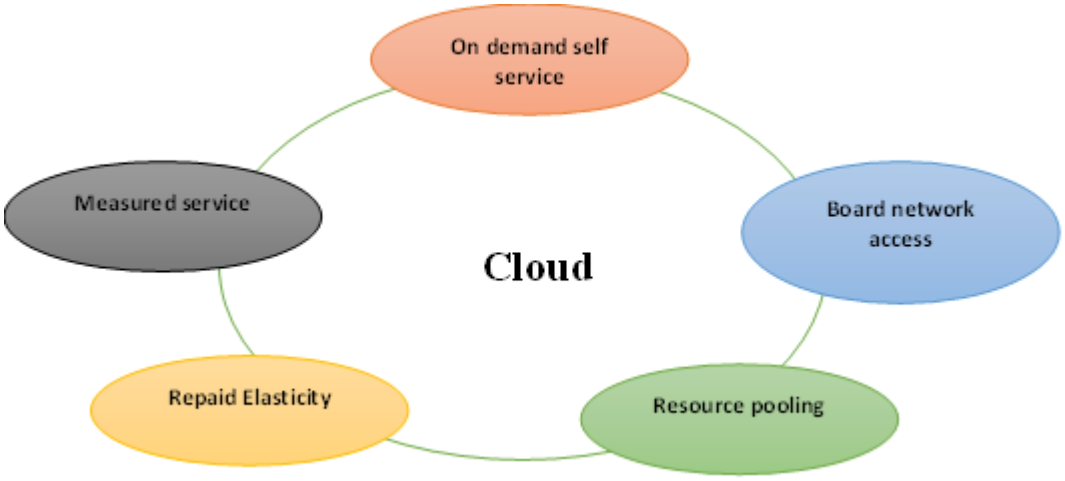

Fig I: Cloud Computing Important Features.

Depending on whether they offer IaaS, SaaS, or PaaS, a cloud provider produces, deploys, and manages the resources, applications, and services in a cloud computing paradigm. The main components for effectively utilizing the already-existing resources and applications are multi-tenancy and virtualization. By utilizing virtualization, a single server, computer facility, data centre, and operating system can host numerous users. This idea of resource sharing allows a cloud provider to service a large number of users [6]. The security concerns brought on by multi-tenancy and virtualization in the cloud context include data protection, communication, resource management for isolation, and virtualization. At any given time, several users share the cloud computing infrastructure. The providers have authority over a common environment where user data is processed and stored [7]. Other malevolent entities may interfere with user data. The need for data privacy and protection in the cloud environment is becoming more important due to factors including lack of transparency on the location of data storage in the cloud environment, regulatory concerns resulting from cross-border storage, etc. Hence, important security concerns in cloud computing revolve around issues related to data protection, such as data confidentiality, integrity, and availability [8].

Users can access pooled IT resources through the Internet in a simple Pay-per-Use-On-Demand manner with cloud computing. Where the network, server, storage, application, service, and other IT resources may be deployed quickly, easily, with the least amount of management, and in conjunction with service providers. IT resource availability can be increased using cloud computing, which also has various advantages over previous types of computing. Customers can use the IT infrastructure in a Pay-per-Use-On-Demand mode, which is advantageous and saves money on purchasing any potentially unused physical resources [9].

So, choosing the right server for data storage and security in this context is essential. Here, the emphasis is on two issues: first, selecting the best cloud data storage server; and second, ensuring data security and preventing unwanted access [10]. The best solution can be found using meta-heuristic approaches which take a rational amount of time. Maximum algorithms were proposed to focus on these issues [11]. With the internet, cloud computing provides consumers with storage options so they can save their data remotely. For both the user and the CSP, remote computing presents a variety of security difficulties and problems. The CSP uses a variety of network technologies while providing its services online, which also raises security concerns. Cloud computing confronts a number of security issues, including shared technology flaws, data breaches, account and service takeovers, DoS attacks, and hostile insiders [12].

What follows is the outline for the rest of the paper. The related work is briefly described in part 2, and the methodology and the theoretical foundations of the methods used are described in section 3. The simulation results and analysis are presented in section 4. For the chapter's final section, "key findings" we summarize the most important results.

2. Previous Related Work

The term "cloud computing" refers to a platform that allows users to share resources in order to gain access to high-quality cloud-based services and applications via the internet. When it comes to the accessibility and storage of data, cloud computing offers a number of advantages [13].

The expansion of cloud computing is being hampered by the growing concern over the privacy of users' data. As a result, safety and privacy are extremely important to the development of cloud computing, despite the fact that they raise a number of difficult challenges. There are several different approaches being considered for protecting users' privacy in cloud computing. This chapter examines a variety of approaches to the privacy protection that is available today [14].

A group of academics came up with remote and local authentication methods for use with wearable technology that is supported by the cloud. The Chebyshev chaotic map and the hash-based selective disclosure technique were presented together as a cooperative effort for the purpose of enabling mutual authentication between the smartphone and the wearable device. Yoking evidence was built to recognise interactions between a smartphone and two wearable gadgets [15], and it was submitted to the cloud server for verification after it was transmitted there. Using a selective disclosure technique that was based on a Merkle hash tree, the goal of this work was to improve the structure of the data field that was contained within the certificate while it was being used for remote authentication. To demonstrate that this protocol adhered to all of the tenets of theoretically sound design, a security analysis was carried out using the Burrows-Abadi-Needham (BAN) logic. This protocol was flexible and could be made available for use with wearable technology, which is always close at hand [16].

Other researchers used computing outsourcing and signal processing techniques from the Compressive Sensing (CS) domain to create an online service for picture reconstruction and identity verification. The image CS samples were uploaded to the cloud for condensed storage. In order to protect privacy, this technology made sure that the cloud rebuilt the image securely without damaging the original content [17]. The cloud then offers the rebuilt service during the management phase based on the outcomes of the identity authentication. The effectiveness of these strategies was examined through theoretical and empirical studies. The analysis' findings demonstrated that this strategy had a manageable computing complexity and satisfactory security performance [18].

The Third Party Medium (TPM) was introduced here for laborious work. In TPM, authenticators were developed for users, and the accuracy of the data was checked for the benefit of users. To protect the privacy of the TPM data, trouble-free procedures were carried out when uploading and auditing the data [19]. Users did not complete the time-consuming decryption operations when using cloud data. The authorization process included the definition of an expiration time to ensure that the TPM who had the authorization could upload the data within the legal time frame. This method's effectiveness was examined, and the security proof was completed. The investigation demonstrated that this technique was effective and extremely secure [20].

Another group of academics unveiled an identity-based group signature-based anonymous authentication method for cloud platforms. The identity-based group signature allowed cloud users to certify that they were free to access cloud data without providing their identities [21]. This method produced an anonymous signature for the group's approval of the user. Although the cloud provider was aware of the authorized group's access, it was not aware of the identities of specific users. Here, the size of the group public key and the signature length varied according to the composition of the group [22]. Once the user joined the group, they were able to sign many messages using the same key pair. This method featured attributes including signer anonymity, traceability, and accuracy. This method has been used in a variety of applications where protecting group identities was important, such as e-commerce, e-voting, and auctions [23].

Further studies have described the architecture for policy-based authorization, which the cloud provider could offer to cloud customers as a service. Users in this case set their own privacy rules. The user's privacy policies are tied to the user's data thanks to the authentication architecture [24]. So, despite the fact that data was transferred between cloud services and cloud providers, policies regulated data access. Also, the authorization infrastructure made sure that different authorities, including the data controller, data issuer, the data subject, and legal, wrote the privacy policies in different policy languages. To resolve disagreements between decisions made by different Policy Decision Points, the authors proposed a conflict resolution mechanism (PDP). This method's performance was examined, and the analysis's findings indicated that it performed well. This approach's flaw is that the PDP produced an overhead [25].

Purpose of the work

(1) To research and evaluate the computational challenges and security concerns that the current approaches confront.
(2) To offer a framework that provides data reliability and a security measure aside from data order, much like how it selects an effective server for data storage.

3. The Proposed Method:

Cloud computing has given users of computational services access to a new, more trustworthy, and more flexible setting that also comes with a guarantee. Here, multiple applications and databases are housed in a single data centre. The primary emphasis of this study is on securing computation and data on the server side, which satisfies the need for safe cloud-based data storage and other safety measures. Figure I is a graphic representation of the security mechanism offered by the twofold authentication technique.

Each time a user logs in to the cloud, a dynamic server requirement is enforced. By combining the Wake Sleep Algorithm and the cuckoo search algorithm, we may achieve a superior outcome in the server selection process. When fitting a multilayer stochastic generative model to high-dimensional data, the wake-sleep technique is a relatively efficient method. In order to approximate the probability distribution across the hidden units given the data, the generative model employs bottom-up connections, which are trained with a straightforward delta algorithm. The idea behind the wake-sleep algorithm is that the system is constantly seeking to refine its internal representation of the world so that it better aligns with external data.

Images of handwritten numerals are just one example of the kind of content the system will try to regenerate during the wake phase from an external source. In contrast, during the sleep phase, the deepest memories draw on their most stable representation of a concept to provide an input that it would also like the system to regenerate from its deeper internal perspective based on the criteria the efficient server is selected, thereby facilitating data storage and access for the user.

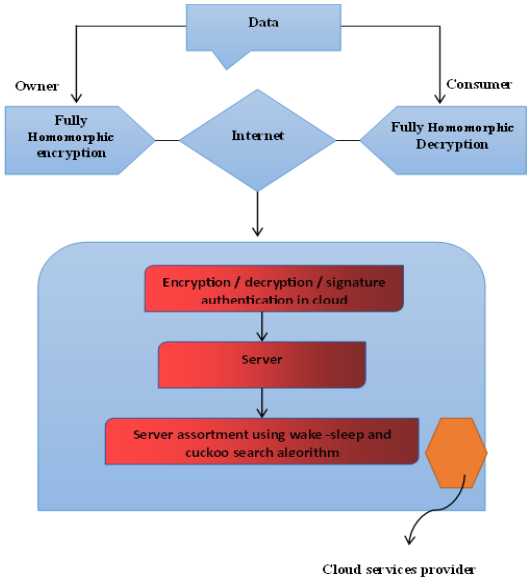

Fig II: The Proposed Algorithm Block Diagram.

We present Wake-Sleep (WS), a straightforward learning system that optimises server selection via a combination of cuckoo search and sleep. To optimise performance, the wake-sleep algorithm switches back and forth between updating the generating model p and the recognition model q. During this time, p (x|z) is being refreshed, also known as the "wake" stage. During the awake phase, we aim to maximise the E [log p (x|z)] of the x-observed data by maximising the z-inferred latent variables. Phase of sleep: maximise E [log q (z; x)] with z as latent. Rather than optimising a single training objective, the Wake-Sleep algorithm switches back and forth between the two. The inability to predict whether or not the algorithm will converge on a satisfactory model of the data is a major drawback for most models of interest.

Inspired by the cuckoo bird's parasitic breeding habit, wherein it lays its eggs in the nests of other bird species, Cuckoo Search is a natural-based optimisation technique. The female cuckoo places her eggs in the nest of a different species, the host bird, whose eggs are quite similar to her own. The cuckoo search algorithm is based on the real-life search approach the cuckoo uses to locate the most suitable host nest in which to lay her egg.

These are the golden rules that best capture the essence of Cuckoo Search algorithm:

- In the first phase, cuckoos choose a nest at random and place a single egg there.
- Second, the best nest with the best egg will be passed down to the next generation.

- Third, given a constant total number of host nests, the host bird has a probability a p of finding a cuckoo's egg.

It's possible to do an infinite number of operations on Fully Homomorphic Encryption (FHE) at any given time. To our knowledge, this is the first practical and realisable FHE system that can calculate any function on encrypted data by evaluating an arbitrarily large number of additions and multiplications. A strong framework for obtaining FHE, it is based on the mathematical concept of ideal-lattices and serves as both a description of the scheme and a guide for its implementation. In this article, we will go over the steps of the fully homomorphic algorithm:

Step 1: The steps for creating a secret key with the FHE technique by picking a random sample.

Step 2: A noise vector is sampled to provide the public key.

Step 3: using the SHMK technique, encrypt the secret key byte by byte.

Step 4: establish the public key.

Step 5: Randomly distribute the samples. Prepare the encrypted message for transmission.

Step 6: decipher each private key. String together the code words and Result from computations.

The Elliptic Curve Digital Signature Algorithm is the elliptic curve implementation of the Digital Signature Algorithm (DSA) (ECDSA). The Elliptic Curve Digital Signature Algorithm, sometimes known as ECDSA, is one of the most well-known representations of elliptic-curve based digital signature protocols. ECDSA has been implemented in hardware in a number of different ways. Nevertheless, because there are so many abstraction levels where the designs can be executed in a variety of ways, it is difficult to compare the work of different developers' concepts.

Computers, ATMs, and smartcards are just a few examples of non-human things that can be authenticated throughout a digital communication process. Hardware solutions for an authentication process are sought after, and they must make do with little in the way of space, runtime, and power because these participants are getting smaller and must be ready to run without large supply units. In this article, we discuss the Elliptic Curve Digital Signature Algorithm, a cutting-edge method for creating and validating digital signatures that meets these requirements (ECDSA).

4. Result and Discussion:

There are potential risks, such as server downtime, hacking, and data corruption. To that end, a server selection framework using fully homomorphic- ECDSA as a double encryption method was developed, and the ensuing experimental findings were discussed.

In Fully homomorphic-ECDSA, the CSP uses the wake-sleep Algorithm with the Cuckoo Algorithm to determine which server will be the most effective. Having chosen a server, the user encrypts their data using completely homomorphic on their end before sending it to the CSP for storage, where it is double-encrypted using ECDSA. This method of double encryption ensures complete privacy on both ends. To ensure data security, privacy, and efficiency, this system combines a server selection method with authentication and encryption techniques. Recent developments in privacy-preserving computation have led to the development of fully homomorphic encryption, which enables operations to be performed directly on cipher text. The information that may be obtained from an accurate decryption is identical to the information that could have been obtained by doing calculations on the data before it was encrypted.

Table I: Execution time analysis and comparison for Fully Homomorphic-ECDSA.

Key Length	**ECIES [5]**		**Fully Homomorphic-ECDSA**	
	Encryption (ms)	**Decryption(ms)**	**Encryption (ms)**	**Decryption (ms)**
160	7.58	7.49	6.18	6.29
256	17.15	16.37	16.57	15.43
384	40.58	38.47	38.46	37.15
512	81.35	82.41	80.19	81.39

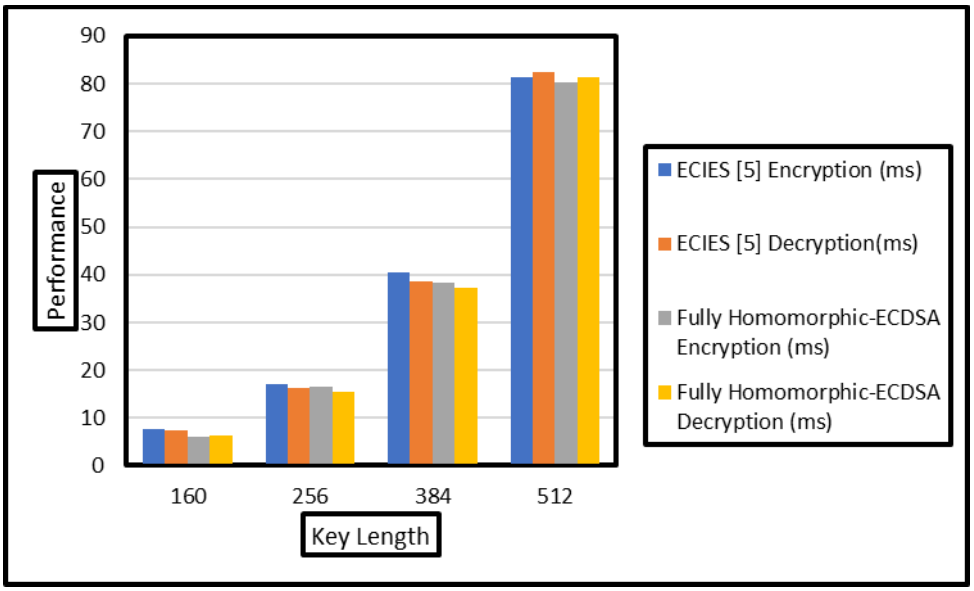

Fig III: Execution time analysis and comparison for Fully Homomorphic-ECDSA.

The procedure for comparing an existing method is laid forth in Table I. The encrypted message in ECDSA is compact because the key size is small compared to ECIES.

Table II: Encryption and Decryption time analysis comparison with different file sizes.

File Size	**RSA [15]**		**Fully Homomorphic-ECDSA**	
	Encryption (ms)	**Decryption(ms)**	**Encryption (ms)**	**Decryption (ms)**
25KB	520	289	348	298
50KB	938	587	459	347
1MB	1524	846	427	357
2MB	1647	873	519	416

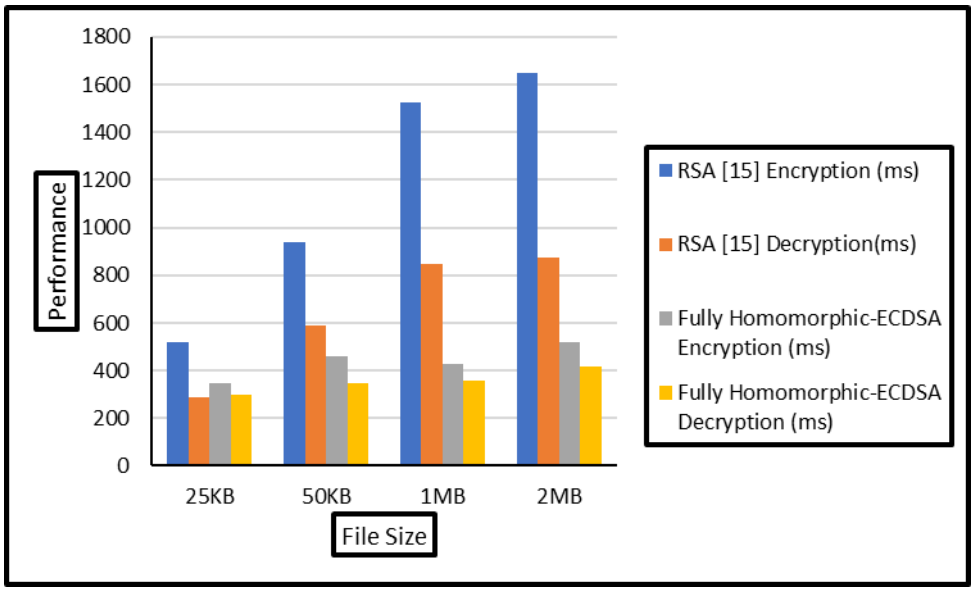

Fig IV: Encryption and Decryption time analysis comparison with different file sizes.

Table II summarises the results of an investigation into how long various known methods take to encrypt and decrypt files of varying sizes. Encryption time is the amount of time needed to go from plaintext to cipher text. The time needed to encrypt a message is proportional to the length of the key, the size of the plaintext blocks, and

the mode. Encryption time was measured in milliseconds in our experiment. The time needed to encrypt data has an effect on how quickly the system can process data. The less time it takes to encrypt data, the faster and more responsive the system will be. Given the data in the table, it is clear that the blowfish technique is the fastest, but it also provides the least secure encryption. Our suggested Fully homomorphic-ECDSA architecture is faster than blowfish while maintaining the same level of security. Decryption time is the amount of time required to convert cipher text back to plaintext. To provide a quick and responsive system, it is preferable that decryption time is significantly less than encryption time. The rate at which data can be decrypted affects the system's efficiency. The deciphering time in our experiment was recorded in milliseconds. Figures III and IV graphically depict how quickly the encryption and decryption processes of blowfish and Fully homomorphic ECDSA, respectively, can be completed. Yet, Figure III shows that Fully homomorphic ECDSA achieves high-level security with average time.

5. Conclusion:

The revolutionary nature of cloud computing, along with the fact that it can significantly reduce the expenses associated with hosting data and is very scalable means that it can improve the capacity to crunch numbers by a factor of many. The advent of cloud computing has freed us from this limitation and decoupled the availability of computing resources from their physical location. As a result, it makes data processing and storage more widely available. As opposed to storing and processing data on a single server in a single location, cloud computing distributes these tasks across a network of remote servers accessible via a central online service. Administration, including data storage and processing, is made possible by the cloud's widespread perception. The primary objective is to probe data security problems and architecture to aid in data security. Similarly to how it selects a server for data storage that is fast, efficient, and uses minimal resources, the system is built to prepare security methods independently of data order. For effective distributed computing with the wake-sleep method, the Cuckoo Search Algorithm (CSA) has been used to select the best available server for the job. Homomorphic encryption, in which data is encrypted before being sent to the server, is used primarily to ensure data authenticity. We've implemented ECDSA encryption on the cloud server to cut down on processing and data storage needs. It improves cloud data security on the end user's device. When all is said and done, the system provides concrete evidence of data privacy, validity, and trustworthiness. Notwithstanding its limitations, this framework does offer secure key communication and data backup services, which are essential for ensuring the privacy of sensitive information stored in the cloud.

Conflict of Interests:

The authors declare that there is no conflict of interests regarding the publication of this paper.

Ethical approval: This article does not contain any studies with human participants or animals performed by any of the authors.

References

[1] Ab Rahman, NH & Choo, KKR 2015, 'A survey of information security incident handling in the cloud', Computers & Security, vol. 49, pp. 45-69.

[2] Abdullah, N, Hakansson, A & Moradian, E 2017, ‗Blockchain based approach to enhance big data authentication in distributed environment', In 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN), IEEE, pp. 887-892.

[3] Acar, A, Aksu, H, Uluagac, AS & Conti, M 2018, ‗A survey on homomorphic encryption schemes: Theory and implementation', ACM Computing Surveys (CSUR), vol. 51, no. 4, pp. 1-35.

[4] Agrawal, N & Tapaswi, S 2019, ‗Defense mechanisms against DDoS attacks in a cloud computing environment: State-of-the-art and research challenges', IEEE Communications Surveys & Tutorials, vol. 21, no. 4, pp. 3769-3795.

[5] Eftekhari, Mahdi & Rostami, Mohamad & Shariatzadeh, Mahdi. (2022). A New Scheme for Image Compression and Encryption Using ECIES, Henon Map, and AEGAN. 10.21203/rs.3.rs-2475241/v1.

[6] Challagidad, PS & Birje, MN 2017, ‗Hierarchical Attribute-based Access Control with Delegation Approach in Cloud', Proceedings of the 11th INDIACom; INDIACom-2017; IEEE Conference ID: 40353 2017 4th International Conference on ‗Computing for Sustainable Global Development', 01st - 03rd March, 2017.

[7] Chandramohan Dhasarathan, Vengattaraman Thirumal & Dhavachelvan Ponnurangam 2017, ‗A secure data privacy preservation for on-demand cloud service,' Journal of King Saud University - Engineering Sciences, vol. 29, no. 2, pp. 144-150.

[8] Chandramohan, D, Vengattaraman, T, Rajaguru, D & Dhavachelvan, P 2016, ‗A new privacy preserving technique for cloud service user endorsement using multi-agents,' Journal of King Saud University - Computer and Information Sciences, vol. 28, no. 1, pp. 37-54.

[9] Chang Guo, QingniShen, Yahui Yang & Zhonghai Wu 2015, ‗User Rank: A User Influence-Based Data Distribution Optimization Method for Privacy Protection in Cloud Storage System,' In Proceedings of the IEEE 39th Annual conference on Computer Software and Applications Conference, pp. 104-109.

[10] K. Latha and T. Sheela, "Block based data security and data distribution on multi cloud environment," Journal of AmbientIntelligence and Humanized Computing, 2019.

[11] T. Joseph, S. A. Kalaiselvan, S. U. Aswathy, R. Radhakrishnan,and A. R. Shamna, "A multimodal biometric authentication scheme based on feature fusion for improving security in cloud environment," Journal of Ambient Intelligence and humanized Computing, vol. 12, no. 6, pp. 6141–6149, 2021.

[12] S. Jarecki, H. Krawczyk, and J. Xu, "OPAQUE: an asymmetricPAKE protocol secure against pre-computation attacks," in Advances in Cryptology – EUROCRYPT 2018, pp. 456–486, Springer International Publishing, Cham, 2018.

[13] D. Wang and P. Wang, "Two birds with one stone: two-factor authentication with security beyond conventional bounds," IEEE Transactions on Dependable and Secure Computing vol. 1. p.1, 2016.

[14] C. Singh and T. D. Singh, "A 3-level multifactor Authentication scheme for cloud computing," International Journal of Computer Engineering &Technology, vol. 10, no. 1,pp. 184–195, 2019.

[15] D. Wang, X. Zhang, Z. Zhang, and P. Wang, "Understanding security failures of multi-factor authentication schemes for multi-server environments," Computers & Security, vol. 88, Article ID 101619, 2020.

[16] S. A. Chaudhry, A. Irshad, K. Yahya, N. Kumar, M. Alazab, and Y. B. Zikria, "Rotating behind privacy: an improved lightweight authentication scheme for cloud-based IoT environment," ACM Transactions on Internet Technology, vol. 21, no. 3, pp. 1–19, 2021.

[17] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, "A robust ECC-based provable secure authentication protocol with privacy-preserving for industrial internet of things," IEEE Transactions on Industrial Informatics, vol. 14, no. 8, pp. 3599–3609, 2018.

[18] C. Wang, D. Wang, G. Xu, and D. He, "Efficient privacy-preserving user authentication scheme with forward secrecy industry 4.0," Science China Information Sciences, vol. 65,no. 1, 2022.

[19] S. Qiu, D. Wang, G. Xu, and S. Kumari, "Practical provably secure three-factor authentication protocol based on extended chaotic-maps for mobile lightweight devices," IEEE Transactions on Dependable and Secure Computing, vol. 1, p. 1,2020.

[20] Q. Jiang, Y. Qian, J. Ma, X. Ma, Q. Cheng, and F. Wei, "User centric three-factor authentication protocol for cloud-assisted wearable devices," International Journal of Communication Systems, vol. 32, no. 6, p. e3900, Article ID e3900, 2019.

[21] M. L. T. Uymatiao and W. E. S. Yu, "Time-based OTP authentication via secure tunnel (TOAST): a mobile TOTP scheme using TLS seed exchange and encrypted offlinekeystore," in Proceedings of the 2014 4th IEEE International Conference on Information Science and Technology, Shenzhen,China, 26 April 2014.

[22] Ometov, S. Bezzateev, N. M¨akitalo, S. Andreev,T. Mikkonen, and Y. Koucheryavy, "Multi-factor authentication: a survey," Cryptography, vol. 2, no. 1, pp. 1–31, 2018.

[23] V. Singh and S. K. Pandey, "Revisiting cloud security threats: replay attack," 2018 4th International Conference on Computing Communication and Automation (ICCCA), in Proceedings of the 2018 4th International Conference on Computing Communication and Automation (ICCCA)Greater, pp. 1–6, Noida, India, 14 December 2018.

[24] S. Kaur and G. Kaur, "Threat and vulnerability analysis of cloud platform: a user perspective," in Proceedings of the 15thINDIACom; INDIACom-2021; IEEE Conference ID: 513482021 8th International Conference on Computing for Sustainable Global Development, pp. 508–514, New Delhi (IN-DIA), 17 March 2021.

[25] F. Ahmet, O. Mustacoglul Ferhat, and C. F. Catak Geoffrey, "Password-based encryption approach for securing sensitive data," Security and Privacy, pp. 1–12, 2020.

[26] Rajesh, P. ., & Kavitha, R. . (2023). An Imperceptible Method to Monitor Human Activity by Using Sensor Data with CNN and Bi-directional LSTM. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2s), 96–105. https://doi.org/10.17762/ijritcc.v11i2s.6033

[27] Dhabliya, D. (2021). An Integrated Optimization Model for Plant Diseases Prediction with Machine Learning Model . Machine Learning Applications in Engineering Education and Management, 1(2), 21–26. Retrieved from http://yashikajournals.com/index.php/mlaeem/article/view/15