



Securing AI-As-A-Service Models Against Sensitive Information Leakage Attacks Based on Lattice Modulated Fully Homomorphism Encryption Algorithm

¹ Nithish Kumar R, ² Seenu K, ³ Nithish M, ⁴ Ashok Kumar,

^{1,2,3} Student, ⁴ Assistant Professor,

Department of Artificial Intelligence and Data Science,

Paavai College of Engineering, Pachal, Namakkal,

Abstract

Security is an important aspect for handling all information through the communication medium in cloud environment which contains sensitive information about the users having personalized information. By handling the security to protect the sensitive data are difficult due to various intrusions created by the attacks to attain data theft, breaches, and false injection with support of cyber threats. By securing the sensitive information is changing and to tackle with Artificial intelligence system to intent advanced cryptography algorithm. To resolve this problem, the research proposes a advanced data verification scheme with intent of Lattice Modulated Fully Homomorphism Encryption Algorithm (LMFHEA) to protect the sensitive information. Initially the sensitive information are prepared for encryption by creating attribute blocks. The blocks contains sensitive information to Create Shuffle Padding Lattice Block With Hash Index Key (SPBK-HI). Then the LMFHEA creates shuffle encryption to create secret key to protect the sensitive information. Finally the Master Proof Authentication Key Principle (MPAKP) validate the secret key from the end user who has authentication rights to allow to decrypt the data. The propose system achieves higher security performance compared to the other system. By validating the security access control, key ensure and integrity principle to ensure the authentication rights and attains improves security parameters potentially they differed from existing methods.

Keywords: Cloud Security, Homomorphic Encryption, Artificial Intelligence, Data Verification, Authentication, Cryptography, Lattice-Based Cryptography.

I. Introduction

The cloud environment has become a ubiquitous platform for storing and processing vast amounts of data, including sensitive user information. This widespread adoption, however, introduces significant security challenges. Protecting sensitive data against theft, breaches, and injection attacks is paramount, especially to counter advanced intrusion techniques. This structure is designed to address ongoing data security and privacy concerns, which remain significant obstacles to businesses looking to adopt cloud services. However, the framework handles large-scale data, multi-tenant environments, or real-time processing, which are important in real-world cloud systems [2].

The application of artificial neural networks (ANNs) in cloud computing security, specifically focusing on their use in intrusion detection systems (IDS). However, this paper does not provide an in-depth evaluation of the effectiveness of ANN-based models in real-world cloud environments [1]. Perimeter-based security models are often insufficient against determined attackers who can penetrate defenses through sophisticated social engineering or zero-day exploits. However, most research does not provide performance data, has unclear scalability, is complex to deploy, and does not discuss compliance [3]. This inherent vulnerability underscores the need for innovative security solutions capable of addressing the dynamic and multifaceted challenges of cloud security. The paper introduces a hybrid homomorphic encryption (HHE) scheme that combines homomorphic encryption to make it more storage—and computation-efficient. However, this could affect storage and communication overhead, especially in bandwidth-constrained environments [4].

This research proposes an advanced data verification scheme that leverages a novel approach based on Lattice Modulated Fully Homomorphic Encryption Algorithm (LMFHEA) to enhance the protection of sensitive information within cloud environments. The scheme incorporates a multi-layered approach to data security, starting with the pre-processing of sensitive data into structured blocks ready for encryption. This initial step involves the creation of attribute blocks, which serve as the fundamental units of data protection. These blocks are then subjected to a Shuffle Padding Lattice Block With Hash Index Key (SPBK-HI) process, further obfuscating the data and enhancing its resistance to unauthorized access.

At the core of the proposed scheme lies the LMFHEA, which provides the cryptographic foundation for secure data handling. The LMFHEA is designed to perform shuffle encryption using a secret key to protect the sensitive information, enabling secure processing and storage significantly reducing the risk of data exposure during processing. To ensure secure access and prevent unauthorized decryption, the scheme incorporates a robust authentication mechanism based on the Master Proof Authentication Key Principle (MPAKP). The MPAKP is responsible for validating the secret key of the end user, ensuring that only authorized individuals with appropriate authentication rights are permitted to decrypt the data.

The proposed system aims to achieve superior security performance compared to existing security mechanisms. The subsequent sections of this research will delve into the specific implementation details of the proposed advanced data verification scheme, including a detailed explanation of the LMFHEA algorithm, the SPBK-HI process, and the MPAKP-based authentication mechanism. Furthermore, a comprehensive evaluation of the system's performance will be presented, demonstrating its effectiveness in protecting sensitive information against various types of attacks. This evaluation will include a comparative analysis against existing security methods, highlighting the advantages of the proposed approach in terms of security, performance, and scalability. By addressing the critical security challenges associated with cloud computing, this research aims to contribute to the development of more secure and trustworthy cloud environments, fostering greater adoption and confidence in this transformative technology.

The contribution and objective of the proposed system is develop an advanced data verification scheme utilizing Artificial Intelligence (AI) driven advanced cryptography, specifically the Lattice Modulated Fully Homomorphic Encryption Algorithm (LMFHEA), to enhance security and data integrity in cloud environments. This proposed system addresses the vulnerabilities inherent in conventional methods and aims to provide a more robust and resilient security architecture.

II. Preliminary surveys

Cloud environments, by their very nature, involve the transmission and storage of user data across shared infrastructure, creating vulnerabilities that are susceptible to a myriad of intrusions, including data theft, breaches, and false injection. These attacks, fueled by increasingly sophisticated cyber threats, necessitate robust security mechanisms to safeguard personalized user information and maintain data integrity. The paper introduces a privacy-preserving Graph Neural Network (GNN) framework called LGA-PGNN, tailored for distributed graph learning where data is spread across multiple data centers and user privacy is a critical concern. However, more sophisticated privacy threats, like membership inference, model inversion, and re-identification attacks, aren't discussed [5]. AI framework that combines Fully Homomorphic Encryption (FHE) for data privacy and security, especially for computations over encrypted

data. However, this introduces a dependency on off-chain systems, which may reduce decentralization and reintroduce trust assumptions [6].

Most studies Optimized Attribute-Based Encryption (ABE)-based access control system for dCloud. However, the ABE still has inherent computational costs; revocation overhead may be significant, and scalability and latency are not detailed [7]. The Parameter optimization framework for TFHE (Fast Fully Homomorphic Encryption over Torus). However, Privacy noise might reduce model accuracy in some cases [8]. However, the proposed scheme may face challenges in scaling to handle large datasets or complex operations in cloud environments, a common problem in homomorphic encryption [9]. Cystography introduces the REDsec framework, which optimizes Fully Homomorphic Encryption (FHE)-based private machine learning inference. However, FHE operations are generally memory-intensive, and the use of ternary networks, while efficient, may still require significant memory resources, especially for larger models [10]. The article addresses the limitations of the revocable-storage identity-based encryption (RS-IBE) scheme proposed by Wei et al., which was designed to support key revocation and ciphertext update functionalities in cloud computing[11]. However, the scalability and complexity of managing keys in larger cloud environments remain potential challenges [12].

The Likelihood Ratio Attack (LiRA), its reliance on low false-positive rates may limit its practical use in some settings, and its performance may vary across different models or as countermeasures evolve [13]. A security framework to ensure privacy and integrity while exchanging sensitive data over cloud or communication systems. However, reliance on trusted authorities and potential scalability concerns in large cloud environments could be drawbacks in certain use cases [14]. The Differential Privacy (DP) and its application to deep learning and federated learning to ensure user privacy. However, the trade-off between privacy and accuracy, scalability, and computational cost concerns remain significant drawbacks [15].

The novel membership inference attack that does not require access to the model's confidence scores (a requirement for previous attacks). However, the defences' scalability and applicability, as well as their computational cost, remain challenges [16]. Cloud computing technologies including AI, data science, blockchain and big data are rapidly integrated into various domains. However, optimizing this process while maintaining security can be a significant hurdle in real-world applications [17].

The abstract discusses optimizing Fully Homomorphic Encryption (FHE) schemes, with a specific focus on reducing the storage complexities associated with the technology, particularly for its use in Internet of Things (IoT) applications. However, the storage reduction might not fully address the scaling needs of complex IoT ecosystems with diverse data types [18]. The secure cloud-edge computing architecture for the Internet of Medical Things (IoMT), which utilizes Fully Homomorphic Encryption (FHE) to address privacy concerns when third-party vendors process sensitive medical data. However, this shows its potential for public health applications and decision-making [19]. The article provides a survey and critical analysis of various data protection and encryption methods used in cloud computing. However, this limits its contribution to practical solutions or innovative methods for tackling cloud security challenges [20].

III. Proposed methodology

The cornerstone of this proposed system is the Lattice Modulated Fully Homomorphic Encryption Algorithm (LMFHEA). The data processing is often outsourced, minimizing the risk of exposing sensitive information to unauthorized parties. The "Lattice Modulated" aspect signifies the use of lattice-based cryptography, known for its resilience against quantum computing attacks, providing future-proof security. LMFHEA leverages the strengths of both FHE and lattice-based cryptography to offer a robust and adaptable encryption solution.

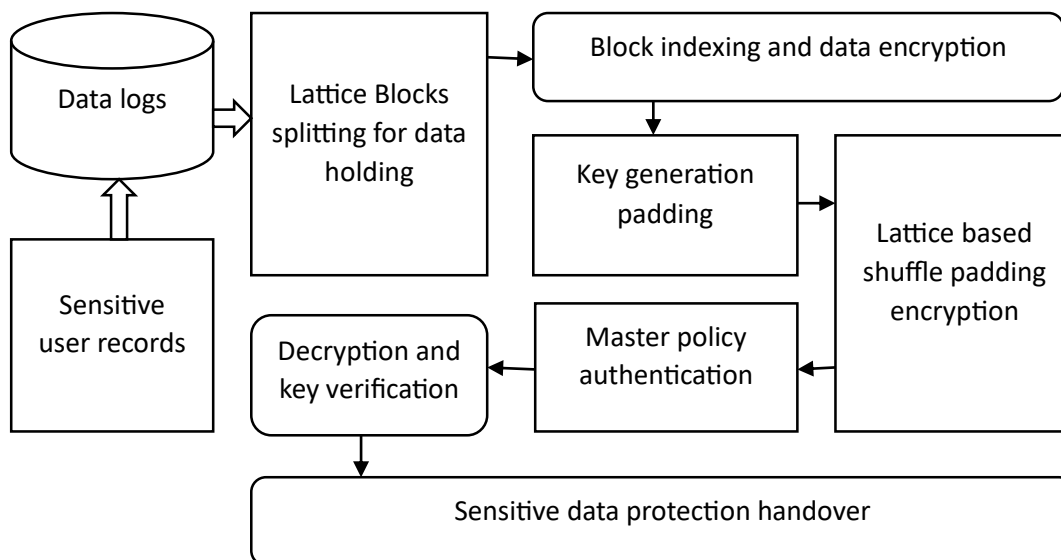


Figure 1: Working principle of LMFHEA algorithm

Before encryption, the sensitive information undergoes a pre-processing phase designed to further obfuscate and enhance security. Figure 1 explains the Working principle of LMFHEA algorithm. This involves breaking down the data into smaller units, termed “artrt8ca blocks.” While the specific details of “artrt8ca blocks” require further elaboration, the intention is to divide the data into manageable segments for easier encryption and manipulation. These blocks are then subjected to a crucial transformation: the creation of Shuffle Padding Lattice Block With Hash Index Key (SPBK-HI). This process introduces several key security enhancements:

- **Shuffling:** The order of the data blocks is randomized through a shuffling algorithm, adding another layer of obfuscation and making it significantly harder for an attacker to reconstruct the original data even if individual blocks are compromised.
- **Padding:** Padding involves adding random, non-sensitive data to each block. This serves two critical purposes. First, it ensures that all blocks are of the same size, preventing attackers from gleaning information based on block length variations. Second, it further obfuscates the actual data within the blocks, making it more challenging to decipher.
- **Lattice Block:** The inclusion of “Lattice Block” suggests that each block is then represented or transformed into a lattice structure, a fundamental element of lattice-based cryptography. This transformation leverages the mathematical properties of lattices to provide strong cryptographic security.
- **Hash Index Key (HI):** Each block is assigned a unique hash index key. This key serves as a pointer or identifier for the block and is crucial for reassembling the data after decryption. The hash function used to generate the key should be cryptographically secure to prevent collisions and ensure the integrity of the index. This also allows for efficient indexing and retrieval of specific data blocks when required.

After the SPBK-HI transformation, the LMFHEA algorithm is applied to create a shuffle encryption with a secret key. The shuffling implemented at the block level is complemented by another layer of shuffling during the encryption process itself. This multi-layered approach makes it extremely difficult to predict the ciphertext based on the plaintext, even with partial knowledge of the encryption process.

A) Blockchain hash index generation

. The blockchain system is distributed among nodes; attackers identify challenges to target and initiate a single-point attack that might be analyzed. Blockchain provides a secure method for healthcare companies to share data because all processes are recorded and arranged chronologically. Then, execute the hash function in equation 1.

$$H(a) = h \quad (1)$$

Here, the medical record's input (a), h is the output of fixed length, and H - hash function. This equation defines a cryptography H that accepts an a and outputs. Creates a secure chain that is connected to the preceding block via a cryptographic technique. Equation 3 is utilized to generate the digital signature D after the block in equation 2 is created. Let's assume (o) –message, E –encryption.

$$D = E_k(H(o)) \quad (2)$$

In this case, o stands for the message, the letter E for encryption, and the letter k for the private key. Using the recipient's matching private key is the sole method to decrypt the message. Once the public key has been encrypted, using equation 5 to verify the chain.

$$U = \prod_{a=1}^n H(B_a) \quad (3)$$

By confirming the hash of every block from 1 to n , this equation 5 determines the validity U of a blockchain

B) Lattice modulated Fully Homomorphic Encryption Algorithm (LMFHEA)

FHE enables the evaluation of cryptographic functions, allowing analysis of encrypted data and binary operations on the corresponding plaintext. Efficient homomorphic evaluation of efficiently computable functions based on FHE techniques consists of four primitives: key generation, encryption, decryption, and re-encryption. Parties use the FHE algorithm to directly access encrypted results without accessing the plaintext. A random "noise vector" is generated by encoding the bits with a public key and determining the Hamming weight of the random noise so that each input has a value of 0 with some probability. Similarly, the re-encryption process is implemented by the homomorphic approximation for the encryption circuit in the cipher. The FHE algorithm then determines a polynomial that implements the encryption process. The central processing unit computes new values, while the graphics processing unit calculates additional values based on the previous iteration. Re-encryption constants are incorporated in the GPU-CPU public key. The public key is correctly encrypted at each iteration, and subsequent coefficients are easily calculated by multiplying the result of the previous iteration.

The computer encodes message bits with a maximum of zeros. Calculate the Hamming weight of random noise as indicated in equation 4. Let's assume f –message bit, h and w – public key, g – ciphertext, $v_m w^m$ –large number of zeros, w –random noise.

$$g = [(f + v(w))]_2 = [f + 2 \sum_{m=1}^{j-1} v_m w^m] \quad (4)$$

As shown in Equation 2, the encrypted data is computed using arithmetic operations and processed directly using modular arithmetic in the cipher. Let's assume E –encryption data, i –modular operation, h –decrypt.

$$\begin{aligned} E(i_1 + i_2) &= (g_1 + g_2) \pmod{h} \\ E(i_1 \cdot i_2) &= (g_1 \cdot g_2) \pmod{h} \end{aligned} \quad (5)$$

Equation 5 shows the estimated cipher bits the computer can recover from the ciphertext. Let's assume w –private key. $i = [g \cdot r]_2 \pmod{2}$. Equation 6 shows that each force is divided into a constant and a random part. The decrypt process is implemented through homomorphic evaluation of the ciphertext

decryption circuit. Let's assume W –constant, m –block, k_m –encode, h –decryption process, t –private key divided into pieces.

$$\begin{aligned} i &= [g.r]_h \bmod 2 \\ &= [\sum^t g p_m w^{k_m}]_h \bmod 2 \\ &= [\sum^t g p_m w^{k_m}]_2 - [(\sum^2 g p_m w^{k_m})/h]_2 \\ &= [\sum^t g p_m w^{k_m}]_2 - [(\sum^2 g p_m w^{k_m})/h]_2 \end{aligned} \quad (6)$$

Equation 5 illustrates the block sum calculation procedure to optimize each encryption vector. Let's assume $k(e, f)$ –corresponding labelled, e and f – two position labels, $\eta_e^{(m)}, \eta_f^{(m)}$ – corresponding encode label.

$$g p_m w^{k_m} = \sum_e \eta_m^{(m)} \sum_f \eta_f^{(m)} g p_m w^{k(e, f)} \quad (7)$$

To assess predictive power, a direct approach to polynomial estimation is used. Calculate the polynomial's window size using the sliding window technique, as illustrated in Equation 8. Let's assume w –window size.

$$\sum(v w^m) = \sum_{n=0}^{s-1} [w^{r.n} \sum_{m=0}^{r-1} (v_m + R_n w^n)] \quad (8)$$

The Fast Fourier Transform (FFT) format is linear, estimates the sum in the FFT domain as demonstrated in Equations 9 and 10. Let's assume w^m –reformulation FFT cost, $IFFT$ –modular reductions,

$$\sum(v w^m) = IFFT(\sum_{n=0}^{j/r-1} [W^{r.n} \cdot \sum_{m=0}^{r-1} (v_{m+r_n} w^m)]) \pmod{h} \quad (9)$$

$$g p_m w^{k_m} = \sum_e \eta_m^{(m)} \sum_f \eta_f^{(m)} g p_m w^{k(e, f)} \quad (10)$$

The most time-consuming part of the basic re-encryption process is processing the blocks and computing their sum. If a block is encoded correctly, the multiplier can easily be calculated from the result of the previous iteration.

The Dynamic random key generation algorithm is a traditional encryption, which relies on a single secret key is created using unique prime numbers, allowing for message encryption. After selecting the public key, the encryption process produces ciphertext.

Algorithm

Input: Keys encrypt messages

Output: plain text from the cipher text CT^e

Start

1. Select two unique prime numbers $\leftarrow x, y$

$$j = x * y$$

2. Select an encryption key $\leftarrow (x - 1), (y - 1)$

3. Select the decryption key

$$(d * e) \bmod (x - 1) * (y - 1) = 1$$

4. Calculate the public key set $\leftarrow \{j, e\}$

5. Calculate the private key set $\leftarrow \{j, d\}$

6. Compute a cipher for plaintext encryption

$$CT = PT^e \bmod j$$

7. Sent to the receiver in a ciphertext $\leftarrow CT$

8. Estimate the plaintext from the ciphertext during decryption

$$CT^e \bmod j$$

Stop

Let's assume CT – ciphertext, d – decryption, e – encryption, PT^e –plaintext, x, y – prime numbers, j –unique numbers.

C) Master Proof Authentication Key Principle (MPAKP)

Finally, the proposed system implements a Master Proof Authentication Key Principle (MPAKP) to validate the secret key. This constitutes a robust authentication mechanism. The MPAKP ensures that only authorized users with the correct authentication rights can decrypt the data. The principle likely relies on a multi-factor authentication process where the user's identity is verified through multiple methods before the secret key is released for decryption. The data handover process in PEMNA can only be completed following successful key verification to maintain data security through multiple layers of protection for sensitive management platforms.

$$A_{req} = (U_i, K_{priv}^{U_i}) \quad (11)$$

To verify identity, the requesting user sends their private key $K_{priv}^{U_i}$ from their account. During this step, verification guarantees authorized personnel exclusive access to sensitive records

The MPAKP serves as a critical control point, preventing unauthorized access to the encrypted data, even if the ciphertext itself is compromised. from exploiting stolen or compromised keys. $V(K_{priv}^{U_i}, PoKS) =$

$$\begin{cases} 1, & \text{if } K_{priv}^{U_i} \in PoKS \\ 0, & \text{otherwise} \end{cases} \quad (12)$$

This principle enhances the overall security posture of the system by adding an additional layer of protection beyond the cryptographic strength of the LMFHEA algorithm. In essence, it prevents malicious actors

$$Access_{decision} = \begin{cases} 1, & \text{if } V(K_{priv}^{U_i}, PoKS) = 1 \text{ and } M_{valid} = 1 \\ 0, & \text{otherwise} \end{cases} \quad (13)$$

The proposed system aims to achieve superior security performance compared to existing methods by integrating several crucial components: strong encryption using LMFHEA, multi-layered obfuscation through shuffle padding and lattice blocks, robust authentication through MPAKP, and integration of AI for continuous monitoring and threat detection. The advantages of this approach are manifold: The proposed system validates security through access control, key assurance, and integrity principles. Access control is managed through the MPAKP, ensuring that only authenticated users with the necessary permissions can access the decryption key. Key assurance is achieved through the use of a cryptographically secure random number generator and the robust key management practices associated with the LMFHEA algorithm. Integrity is maintained through the hash index key, allowing for verification of the data's authenticity.

IV. Result and discussion

The section explored performance evaluation for posed system done with AWS IAM role user simulated with 300 users with personalize sensitive records to make validation and authentication. They require effective methods for assessing healthcare performance. This can really help improve patient care and services.. Additionally, a key authentication mechanism is implemented during the analysis to protect data confidentiality and privacy. Healthcare systems could benefit from this strategy by deploying a secure and scalable system for data processing and evaluation. The performance of the suggested approach

LMFHEA and the current methodologies ABS, RS-IBE, and FHE are contrasted in the sections that follow. Healthcare data is protected during transmission and storage by encryption and decryption. The process of converting data into a secure format is called encryption, and the process of converting it back into an understandable format is called decryption. It takes time for basic medical data to be converted into ciphertext and vice versa.

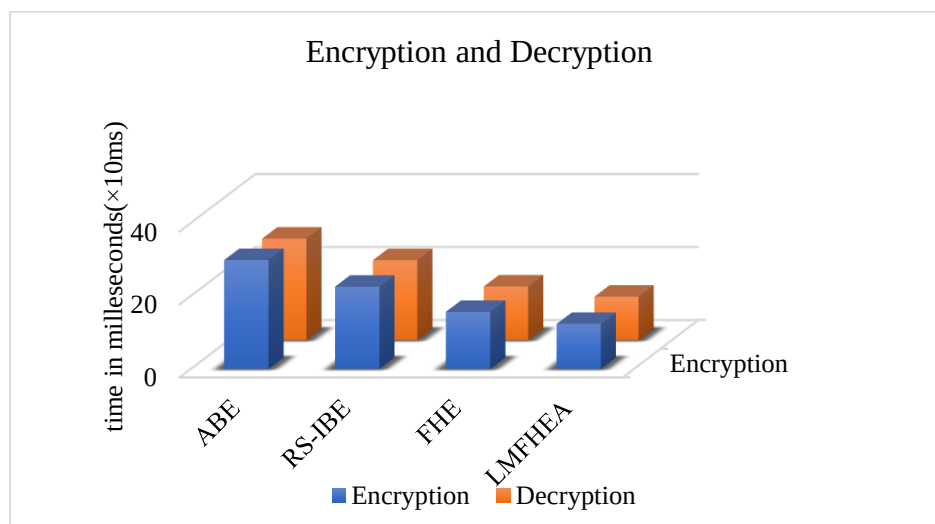


Figure 2: Encryption and Decryption Analysis

Figure 2 shows that the PHR dataset to carry out the encryption and decryption operation. Data encryption and decryption using the LMFHEA method take 12.3ms and 11.9 ms, respectively. Because of this, LMFHEA demonstrates quicker encryption and decryption times than current techniques.

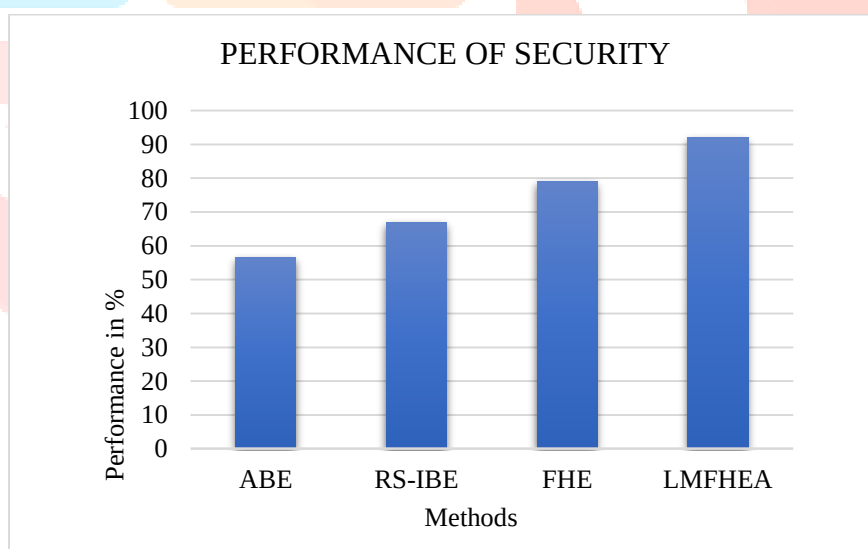


Figure 3: Analysis of Security performance

Figure 3 shows the results of the security analysis using the sensitive dataset. With a security performance of 92.1%, the LMFHEA outperforms other approaches. By using blockchain technology and improved privacy-preserving approaches, LMFHEA enhances security while keeping computing complexity low.

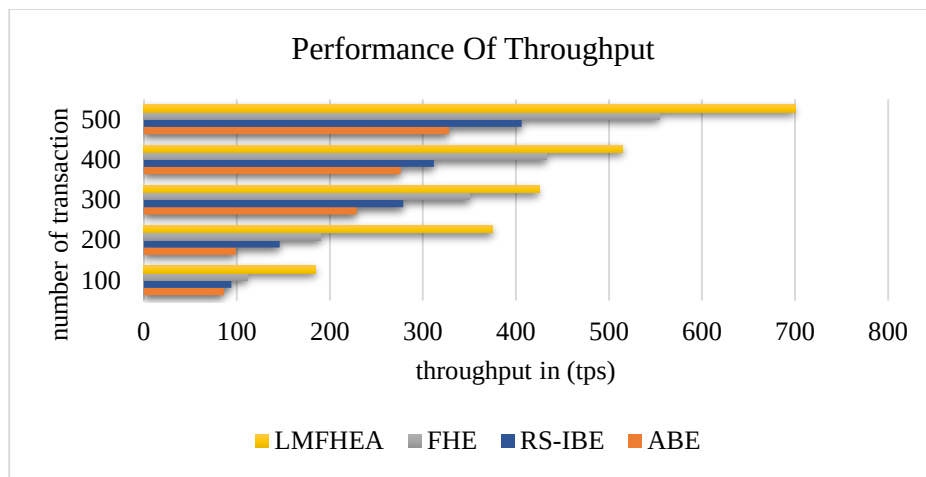


Figure 4: Analysis of throughput performance in (TPS)

Figure 4 shows the analysis of LMFHEA throughput performance using the sensitive dataset and current techniques. When compared to current approaches, the LMFHEA transaction performance offers a 700 transmission per second (tps) greater rate. By simplifying encryption and streamlining data processing via blockchain, LAES increases throughput.

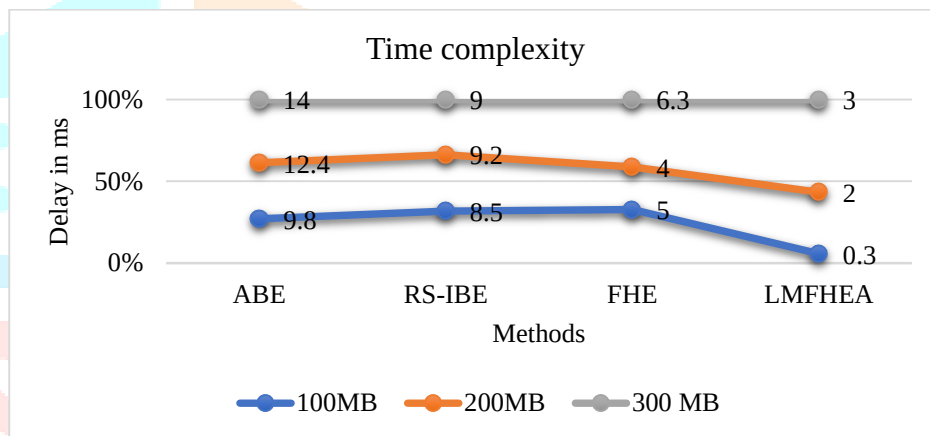


Figure 5: Analysis of Delay in (ms)

Figure 5 shows that, in comparison to a typical crypto blockchain, the LMFHEA results in a 2 millisecond (ms) reduction in authentication delay for 300 MB of data. The suggested system outperforms the conventional crypto blockchain in terms of higher-end security and authentication latency.

V. Conclusion

In conclusion, this advanced data verification scheme, with its innovative combination of Lattice Modulated Fully Homomorphic Encryption, shuffle padding, lattice blocks, hash index keys, and the Master Proof Authentication Key Principle, offers a compelling solution to the challenges of securing sensitive information in cloud environments. By addressing the vulnerabilities inherent in traditional methods and incorporating advanced cryptographic techniques, this LMFHEA system provides a robust and resilient security architecture that can effectively protect against a wide range of cyber threats and improve security parameters that differ potentially from existing methods. Further research and development are needed to refine and optimize the implementation of this system, but its potential to revolutionize data security in the cloud is undeniable. Furthermore, incorporating AI-driven threat detection and anomaly detection systems would further strengthen the security posture of this proposed system, enabling it to proactively identify and respond to potential threats. The future of cloud security relies on innovations like this, which prioritize data confidentiality, integrity, and availability in the face of ever-evolving cyber threats.

Reference

1. S. L. Nita and M. I. Mihailescu, "On Artificial Neural Network used in Cloud Computing Security - A Survey," *2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, Iasi, Romania, 2018, pp. 1-6, doi: 10.1109/ECAI.2018.8679086.
2. Haifaa Jassim Muhasin, R. Atan, M. b. A. Jabar and Salfarina binti Abdullah, "Cloud computing sensitive data protection using multi layered approach," *2016 2nd International Conference on Science in Information Technology (ICSITech)*, Balikpapan, Indonesia, 2016, pp. 69-73, doi: 10.1109/ICSITech.2016.7852610.
3. Xinhua Dong, Ruixuan Li, Heng He, Wanwan Zhou, Zhengyuan Xue and Hao Wu, "Secure sensitive data sharing on a big data platform," in *Tsinghua Science and Technology*, vol. 20, no. 1, pp. 72-80, Feb. 2015, doi: 10.1109/TST.2015.7040516.
4. J. H. Cheon and J. Kim, "A Hybrid Scheme of Public-Key Encryption and Somewhat Homomorphic Encryption," in *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 5, pp. 1052-1063, May 2015, doi: 10.1109/TIFS.2015.2398359.
5. X. Pei, X. Deng, S. Tian, J. Liu and K. Xue, "Privacy-enhanced graph neural network for decentralized local graphs", *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 1614-1629, 2024.
6. P. -C. Chen, T. -H. Kuo and J. -L. Wu, "A Study of the Applicability of Ideal Lattice-Based Fully Homomorphic Encryption Scheme to Ethereum Blockchain," in *IEEE Systems Journal*, vol. 15, no. 2, pp. 1528-1539, June 2021, doi: 10.1109/JSYST.2021.3064053.
7. Y. Liang *et al.*, "Research of Access Control System Based on Attribute Encryption Technology that Suitable for Dispatching and Control Cloud," *2019 IEEE 4th International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)*, Chengdu, China, 2019, pp. 358-362, doi: 10.1109/ICCCBDA.2019.8725782.
8. L. Bergerat, A. Boudi, Q. Bourgerie, I. Chillotti, D. Ligier, J.-B. Orfila, et al., "Parameter Optimization and Larger Precision for (T)FHE", *Journal of Cryptology*, vol. 36, no. 3, pp. 28, Jun. 2023.
9. R. C. R, P. S. Harshini, T. N, C. T. R and D. B. Srinivas, "A Multi-Stage Partial Homomorphic Encryption Scheme for Secure Data Processing in Cloud Computing," *2023 2nd International Conference on Edge Computing and Applications (ICECAA)*, Namakkal, India, 2023, pp. 58-62, doi: 10.1109/ICECAA58104.2023.1021215
10. L. Folkerts, C. Gouert and N. G. Tsoutsos, "REDsec: Running Encrypted Discretized Neural Networks in Seconds", *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, March 2023.
11. K. Lee, "Comments on "Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption", in *IEEE Transactions on Cloud Computing*, vol. 8, no. 4, pp. 1299-1300, 1 Oct.-Dec. 2020, doi: 10.1109/TCC.2020.2973623.
12. O. A. Khashan, "Secure Outsourcing and Sharing of Cloud Data Using a User-Side Encrypted File System," in *IEEE Access*, vol. 8, pp. 210855-210867, 2020, doi: 10.1109/ACCESS.2020.3039163.
13. N Carlini, S Chien, M Nasr et al., "Membership inference attacks from first principles[C]", 2022 IEEE Symposium on Security and Privacy (SP), pp. 1897-1914, 2022.
14. P. More, S. Chandugade, S. M. S. Rafiq and P. Pise, "Hybrid Encryption Techniques for Secure Sharing of a Sensitive Data for Banking Systems Over Cloud," *2018 International Conference On Advances in Communication and Computing Technology (ICACCT)*, Sangamner, India, 2018, pp. 93-96, doi: 10.1109/ICACCT.2018.8529545.
15. A El Ouadrhiri and A Abdelhadi, "Differential privacy for deep and federated learning: A survey[J]", *IEEE access*, vol. 10, pp. 22359-22380, 2022.
16. C A Choquette-Choo, F Tramer, N Carlini et al., "Label-only membership inference attacks[C]", *International conference on machine learning*, pp. 1964-1974, 2021.
17. Dalmo Stutz; Joaquim T. Assis; Asif A. Laghari; Abdullah A. Khan; Nikolaos Andreopoulos; Andrey Terziev; Anand Deshpande; Dhanashree Kulkarni; Edwiges G.H. Grata, "Enhancing Security in

- Cloud Computing Using Artificial Intelligence (AI)," in *Applying Artificial Intelligence in Cybersecurity Analytics and Cyber Threat Detection*, Wiley, 2024, pp.179-220, doi: 10.1002/9781394196470.ch11.
18. W. -T. Song, W. Zhang, D. Tang and B. Hu, "A Small-Size FHE Scheme for Better Privacy Protection of IoT," in *IEEE Internet of Things Journal*, vol. 11, no. 7, pp. 12909-12917, 1 April, 2024, doi: 10.1109/JIOT.2023.3336158.
19. L. Zhang, X. Wang, J. Wang, R. Pung, H. Wang and K. -Y. Lam, "An Efficient FHE-Enabled Secure Cloud-Edge Computing Architecture for IoMT Data Protection With its Application to Pandemic Modeling," in *IEEE Internet of Things Journal*, vol. 11, no. 9, pp. 15272-15284, 1 May, 2024, doi: 10.1109/JIOT.2023.3348122.
20. M. R. Kumar, I. J. S. Jeya and S. Athira, "Analysis of Encryption Techniques for Secure Data in Cloud Environment," *2025 International Conference on Intelligent Systems and Computational Networks (ICISCN)*, Bidar, India, 2025, pp. 1-4, doi: 10.1109/ICISCN64258.2025.10934711.

