Baharon, MR, Yahaya, SH, AlShannaq, O, Shah, HNM and MacDermott, Á

Secure industrial Iot data aggregation in the manufacturing industry using lightweight homomorphic encryption scheme

http://researchonline.ljmu.ac.uk/id/eprint/25528/

Article

SECURE INDUSTRIAL IOT DATA AGGREGATION IN THE MANUFACTURING INDUSTRY USING LIGHTWEIGHT HOMOMORPHIC ENCRYPTION SCHEME

M.R. Baharon[1*], S.H. Yahaya[2], O. AlShannaq[1], H.N. Mohd Shah[3] and A. MacDermott[4]

[1]Fakulti Teknologi Maklumat dan Komunikasi,
Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian
Tunggal, Melaka, Malaysia.

[2]Fakulti Teknologi dan Kejuruteraan Industri dan Pembuatan,
Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian
Tunggal, Melaka, Malaysia.

[3]Fakulti Teknologi dan Kejuruteraan Elektrik,
Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian
Tunggal, Melaka, Malaysia.

[4]Department of Computer Science,
Liverpool John Moores University, L3 3AF, Liverpool, United Kingdom.

*Corresponding Author's Email: mohd.rizuan@utem.edu.my

Article History: Received 16 May 2024; Revised 4 November 2024; Accepted 25 November 2024

ABSTRACT: The rise of the Industrial Internet of Things (IIoT) has revolutionised manufacturing by enhancing efficiency, automation, and data-driven decision-making. However, this advancement presents serious security and privacy challenges, particularly concerning data leaks and unauthorised access. The extensive data sharing among IIoT devices increases their susceptibility to security breaches, which could expose sensitive information and result in financial and physical harm. Moreover, IIoT devices often face resource constraints, such as limited computational power, memory, and battery life, which complicates the implementation of robust security measures. This study focuses on data leakage, unauthorised access, and cyber risks to examine the security issues inherent in IIoT systems. Additionally, it also examined the effect of resource constraints and privacy concerns on the integration of IIoT with Industry 4.0. Recent studies have proposed various solutions to enhance data security and integrity, including homomorphic encryption and blockchain frameworks. In response, this study proposed a novel lightweight homomorphic encryption scheme to address critical vulnerabilities and improve overall security in industrial systems. The encryption scheme was designed and rigorously tested as part of this approach, with findings demonstrating significant improvements in data privacy and system efficiency. The results underscore the importance of robust security measures to ensure the safe and reliable operation of IIoT systems.

KEYWORDS: *Homomorphic Encryption; IIoT; Data Security; Data Integrity; Data Privacy*

1.0 INTRODUCTION

With the advent of Industrial Internet of Things (IIoT), industry has witnessed a dramatic increase in productivity, automation, and data-driven decision-making [1]. Figure 1 illustrates how IIoT is utilised in the manufacturing sector. However, there are significant security and privacy issues with this technological advancement that require our attention in order to ensure the IIoT systems operate safely and dependably. A major concern is the risk of unauthorised access and data leakage [2]. The vast volume of data exchanged among IIoT devices makes them vulnerable to breaches, potentially exposing sensitive information, causing financial loss, and even jeopardizing physical safety [3, 4]. Additionally, resource constraints pose a challenge, as IIoT devices often struggle with limited memory, processing power, and battery life [5, 6]. Implementing robust security measures is difficult under these constraints, thereby exposing systems to potential risks [7].

The primary goal of this study was to investigate the security issues associated with IIoT systems. Specifically, issues such as unauthorised access and data leakage within IIoT environments were addressed. Moreover, the study examined privacy issues and resource constraints related to incorporating IIoT into Industry 4.0. Ultimately, the study sought to enhance the safety and reliability of IIoT operations.

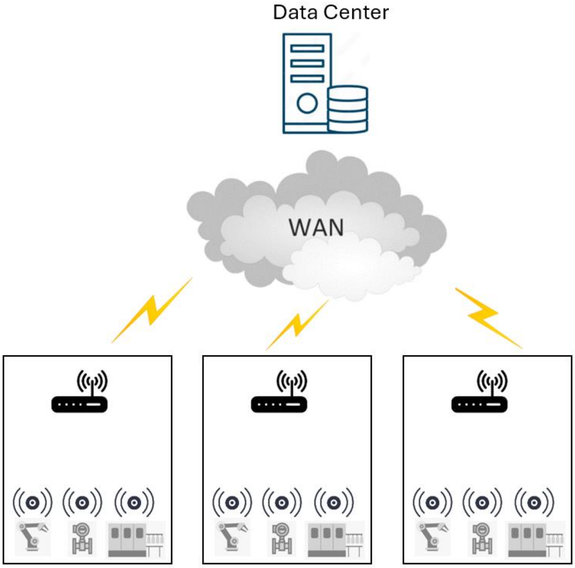


Figure 1: IIoT Infrastructure in Manufacturing Industry.

Several recent studies focused on data security and integrity in the IIoT manufacturing sector using a safe and verifiable Hyperledger Fabric Modular (HFM) architecture [8]. Juma et al. [9] proposed a Trusted Consortium Blockchain (TCB) framework to guarantee data integrity while addressing the challenges of peer validation and real-time transaction monitoring in IIoT infrastructures. Furthermore, a homomorphic encryption method was introduced by Alqahtani et al. [10] with an emphasis on optical fibre communication, to improve data security and privacy in IoT contexts. The study emphasised the reduction of encryption length and improvements to data security during storage. Moreover, a novel concept of security against a verified Chosen-Ciphertext Attack (vCCA) was introduced by Manulis and Nguyen [11], who focused on developing fully homomorphic encryption (FHE) schemes that accomplish adaptive chosen-ciphertext security.

In view of the importance of research on data security and integrity research in IIoT manufacturing, a novel lightweight homomorphic encryption scheme has been proposed. By addressing major vulnerabilities, this scheme aims to improve the overall security posture of industrial systems and mitigate significant risks. Resource constraints such as computational power and storage have been carefully considered. Implementing homomorphic encryption ensures the privacy and integrity of aggregated data while maintaining its security. Such a scheme can significantly enhance the efficiency of IIoT, as computational constraints remain a primary concern. This innovative approach addresses the pressing need for secure data aggregation in the manufacturing, marking a substantial advancement in the field.

The remainder of the paper is structured as follows: Section 2 outlines the methodology of the proposed scheme. Section 3 presents the results and discussion. Finally, the conclusion is provided in Section 4.

2.0 METHODOLOGY

This section describes the proposed lightweight homomorphic encryption scheme. The scheme comprised four algorithms, namely, key generation, data encryption, data processing and data recovery. For implementing such algorithms in an Industrial IoT (IIoT) System, several parameters were set beforehand and described as follows. Suppose that there are n sensor nodes in the IIoT network, each of which is denoted as $u_i(1 \leq i \leq n)$. In addition, the maximum length of each data item to be computed is set to τ bits. In such a network, several Data Aggregators (DA) are employed to calculate the received sensor data from the n sensor nodes. Furthermore, two functions are defined for data processing. Moreover, a client-server structure is implemented to represent the sensor nodes and their connections as links. Finally, the connected sensor nodes were presumed to have already authenticated one another and, if necessary, created a secure communication channel.

In the key generation process, a symmetric secret key was employed for data encryption by each sensor node, u_i. Each sensor node, u_i used a unique secret key generated and was published by Data Aggregator, DA for symmetric data encryption. The encrypted data was then outsourced to the Cloud Server, CS via the DA for data processing. This phase allowed all the sensor nodes to submit their sensing data to the CS in an encrypted form. The DA aggregated all the received sensor data before transmitting it to the aggregation server for verification purposes. Finally, the data center recovered the results without knowing any individual values transmitted by different nodes. Figure 2 describes the algorithms executed by the data aggregator, sensor nodes, Cloud Server and the data center.

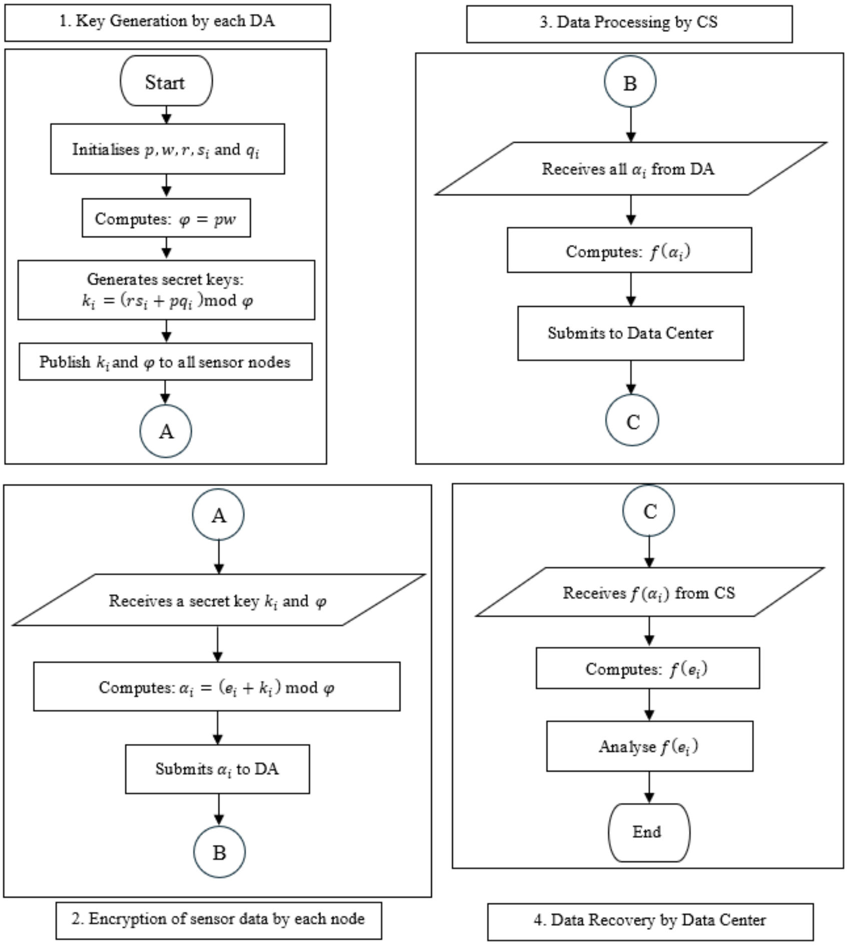

1. Key Generation by each DA
Start
Initialises p, w, r, s_i and q_i
Computes: $\varphi = pw$
Generates secret keys:
$k_i = (rs_i + pq_i) \bmod \varphi$
Publish k_i and φ to all sensor nodes
A
3. Data Processing by CS
B
Receives all α_i from DA
Computes: $f(\alpha_i)$
Submits to Data Center
C
A
Receives a secret key k_i and φ
Computes: $\alpha_i = (e_i + k_i) \bmod \varphi$
Submits α_i to DA
B
2. Encryption of sensor data by each node
C
Receives $f(\alpha_i)$ from CS
Computes: $f(e_i)$
Analyse $f(e_i)$
End
4. Data Recovery by Data Center

Figure 2: The proposed Lightweight Homomorphic Encryption Scheme

3.0 RESULTS AND DISCUSSION

In this section, an IIoT infrastructure simulation was executed to gauge how well the IIoT devices implemented the proposed scheme. As demonstrated in Figure 3, sensor nodes were distributed randomly and connected to the Data Aggregator via a wireless connection. Key generation, data encryption, data processing, and data recovery were all included in the evaluation of the delay incurred during a single round of data processing. The delays in completing a single round of data processing were measured by using two functions by a CS.

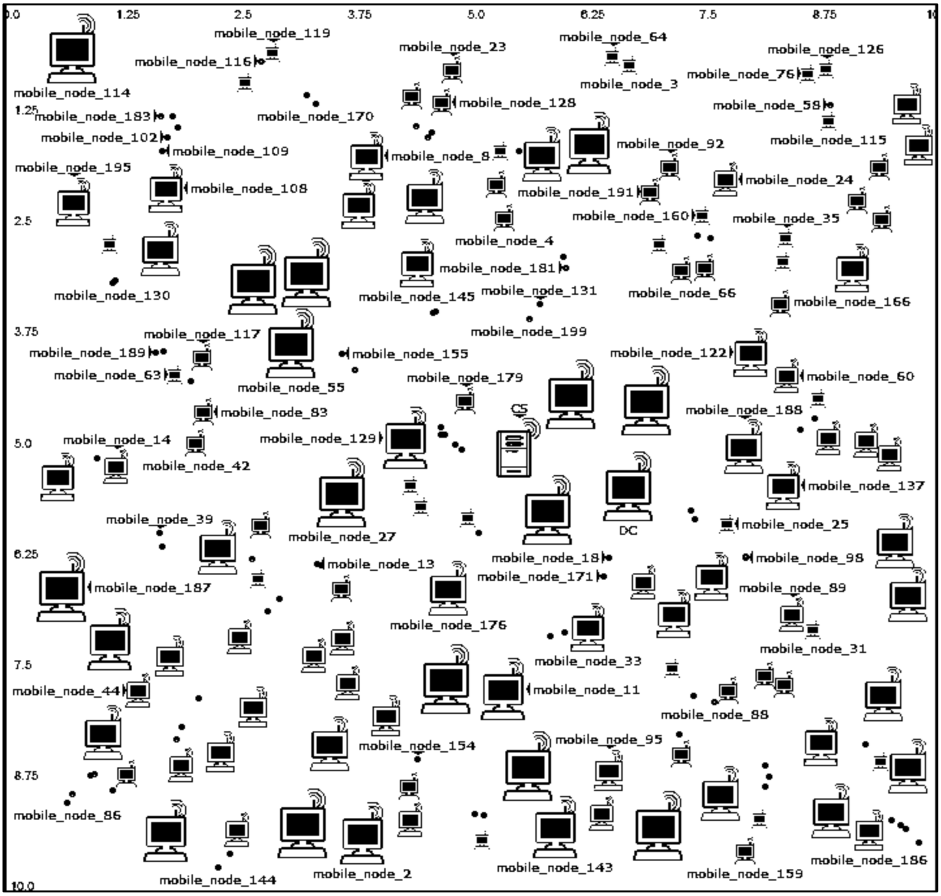


Figure 3: Simulation of IIoT using OPNET

For the security analysis, several algorithms were compared to highlight the state-of-the-art performance of the proposed algorithm.

Each requirement (Data Integrity, Data Privacy, Data Confidentiality, and Data Availability) had been examined before comparing the security needs for the given algorithms based on the algorithms' characteristics and strengths. The results are shown in Figure 4.

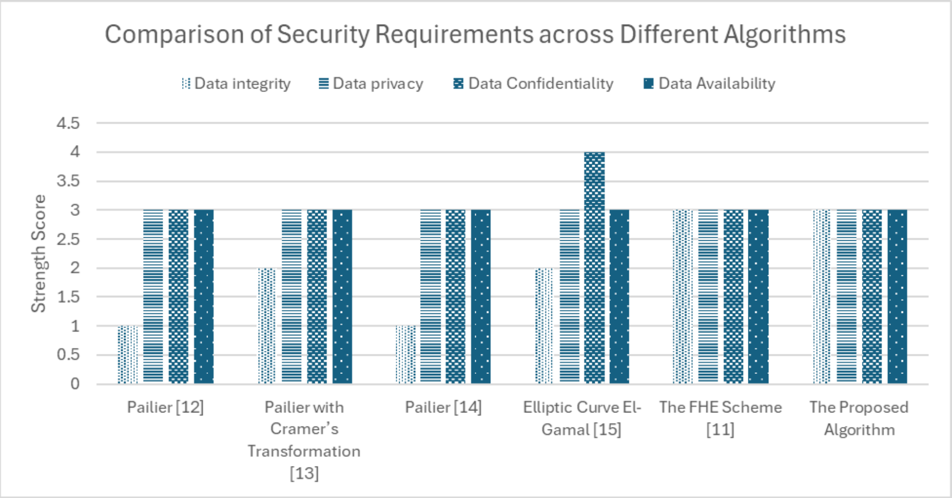
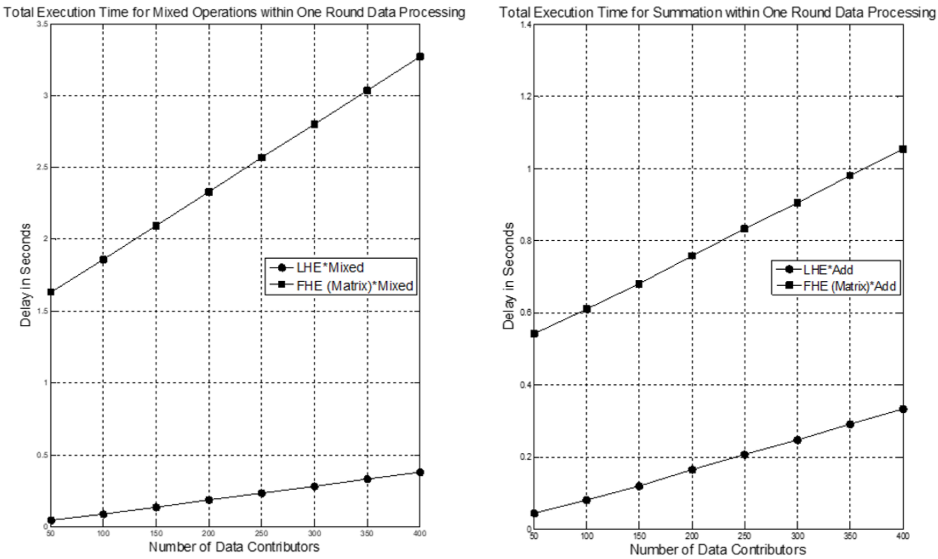


Figure 4: The Comparison of Security Requirements

For IIoT infrastructure in manufacturing, Paillier and Paillier with Cramer's Transformation offers strong privacy and confidentiality but requires additional mechanisms for data integrity and may have performance overhead impacting availability [12, 13]. Furthermore, Paillier Cramer-Shoup improves upon the basic Paillier by incorporating data integrity and providing robust security against a broader range of attacks, despite its higher computational complexity [14]. Moreover, EC El-Gamal excels in providing very strong privacy and confidentiality with efficient performance, but its data integrity score is moderate [15]. In contrast, FHE and the proposed scheme are more suitable for implementation as they support all the security requirements with balanced scores.

To determine the most suitable algorithm for IIoT infrastructure in manufacturing implementations, both schemes were further evaluated to assess their efficiency in terms of computational performance. Theoretically, the proposed scheme outperformed the FHE scheme in terms of speed, as its computational complexity was higher. Additionally, the overall size of ciphertext data transmitted from the DA to the CS was smaller for the proposed scheme compared to the FHE scheme. This is because, in the FHE scheme, data is represented as a 4 × 4 matrix, meaning that transmitting a single ciphertext requires the transmission of 16 matrix elements [16]. Such data representation results in increased delays, along with higher bandwidth and storage requirements. The experimental results, which measured the delay for both schemes, were compared to evaluate their efficiency. The comparison focused on data summation and combined operations of summation and multiplication within a single round of data processing. The results are presented in Figure 5(a) for data summation and Figure 5(b) for combined summation and multiplication. The delay was measured based on the process illustrated in Figure 1, where four parties communicated to process data in its ciphertext form.


Total Execution Time for Mixed Operations within One Round Data Processing

Total Execution Time for Summation within One Round Data Processing

(a) (b)

Figure 5: The delay incurred during a single round of data processing

Figures 5(a) and 5(b) illustrate the delay incurred during a single round of data processing on the ciphertext for two encryption schemes. The disparity between the two lines demonstrated that the delay introduced by the proposed scheme gradually increased as the number of sensors grew. Nevertheless, the delay associated with the FHE scheme was consistently over 50% higher than that of the proposed scheme and continued to rise as the number of sensor nodes increased. This discrepancy can be attributed to the fact that the compared scheme employs an encryption algorithm involving the matrix multiplication of keys and data. Such computations introduced additional delays due to their cubic complexity, which must be performed by each sensor prior to data processing. Moreover, transmitting ciphertext in matrix form from resource-constrained devices with limited data rates and buffer size capacities necessitated greater bandwidth, thereby compounding the delay in data processing. In contrast, the proposed scheme transmits ciphertext as a single integer, which requires significantly less bandwidth. Consequently, the transmission process is faster, reducing the overall delay for data processing in comparison to the FHE scheme.

4.0 CONCLUSION

In conclusion, while the Industrial Internet of Things (IIoT) has significantly enhanced automation and manufacturing efficiency, it also introduces serious security and privacy challenges. This study highlights the difficulties posed by resource limitations in implementing effective security measures, as well as critical issues such as data leakage, unauthorised access, and cyber threats. An examination of the integration of IIoT within Industry 4.0 reveals that the widespread use of interconnected devices increases vulnerabilities, potentially leading to severe consequences. The proposed lightweight homomorphic encryption scheme offers a viable solution, addressing key vulnerabilities and enhancing data privacy and system efficiency. The positive outcomes of testing this scheme underscore the crucial need for robust security protocols to maintain the IIoT systems integrity and reliability. As IIoT advances, ensuring comprehensive security measures is essential for the safe and sustainable development of industrial operations.

ACKNOWLEDGMENTS

This work has been supported by Universiti Teknikal Malaysia Melaka. The author would like to express gratitude to the Center for Research and Innovation Management (CRIM) UTeM for the continuous support of this work.

AUTHOR CONTRIBUTIONS

M.R. Baharon: Conceptualization, Methodology, Writing-Original Draft Preparation; S. H. Yahaya: Methodology, Writing-Original Draft Preparation; O. AlSyannaq: Conceptualization, Data Validation; H. N. Mohd Shah: Writing-Reviewing, Editing; A. MacDermott: Editing.

CONFLICTS OF INTEREST

The manuscript has not been published elsewhere and is not under consideration by other journals. All authors have approved the review, agree with its submission and declare no conflict of interest on the manuscript.

REFERENCES

[1] N. M. Khushairi, N. A. Emran, and M. M. Yusof, “Query Rewriting using Multitier Materialized Views for Cyber Manufacturing Reporting”, *Journal of Advanced Manufacturing Technology*, vol. 12, no. 1(1), pp. 393-408, 2018.

[2] J. Smith and R. Johnson, "Security Challenges in Industrial Internet of Things (IIoT) Systems", *Journal of Cybersecurity and Privacy*, vol. 10, no. 2, pp. 123-140, 2023.

[3] A. Brown and C. Lee, "Privacy Implications of IIoT Integration with Industry 4.0", in *International Conference on Data Privacy and Security*, 2024, pp. 45-58.

[4] M. Garcia and S. Patel, "Resource-Constrained Security Measures for IIoT Devices", *IEEE Transactions on Industrial Informatics*, vol. 32, no. 4, pp. 567-580, 2025.

[5] S. Pal and Z. Jadidi, "Analysis of Security Issues and Countermeasures for the Industrial Internet of Things", *Applied Sciences*, vol. 11, no. 20, pp. 1-33, 2021.

[6] S. C. Vetrivel, R. Maheswari, and T. P. Saravanan, "Industrial IOT: Security Threats and Counter Measures", in *Communication Technologies and Security Challenges in IoT*, A. Prasad, T. P. Singh, and S. Dwivedi Sharma, Eds. Singapore: Springer, 2024, pp 403–425.

[7] Y. Bobde et al., "Enhancing Industrial IoT Network Security through Blockchain Integration", *Electronics*, vol. 13, no. 4, p. 687, 2024.

[8] R. Kumar, B. Kandpal and V. Ahmad, "Industrial IoT (IIOT): Security Threats and Countermeasures", in *International Conference on Innovative Data Communication Technologies and Application (ICIDCA)*, Uttarakhand, India, 2023, pp. 829-833.

[9] M. Juma, F. Alattar, and B. Touqan, "Securing Big Data Integrity for Industrial IoT in Smart Manufacturing Based on the Trusted Consortium Blockchain (TCB)", *IoT*, vol. 4, no. 1, pp. 27-55, 2023.

[10] A. S. Alqahtani, Y. Trabelsi, P. Ezhilarasi, et al., "Homomorphic encryption algorithm providing security and privacy for IoT with optical fiber communication", *Optical and Quantum Electron*, vol. 56, p. 487, pp. 1-19, 2024.

[11] M. Manulis and J. Nguyen, "Fully Homomorphic Encryption Beyond IND-CCA1 Security: Integrity Through Verifiability", In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, M. Joye and G. Leander, Eds. Cham: Springer, 2024, pp. 63-69.

[12] P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes", in *Advances in Cryptology - EUROCRYPT '99*, Berlin, Heidelberg: Springer, 1999, pp. 223-238.

[13] R. Cramer and V. Shoup, "Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption", in *Advances in Cryptology - EUROCRYPT 2002*, Berlin, Heidelberg: Springer, 2002, pp. 45-64.

[14] R. Cramer and V. Shoup, "A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack", in *Advances in Cryptology - CRYPTO '98*, Berlin, Heidelberg: Springer, 1998, pp. 13-25.

[15] N. Koblitz, "Elliptic Curve Cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203-209, 1987.

[16] A. A. Ahmed, M. M. Madboly, and S. K. Guirguis, "Securing Data Transmission and Privacy-Preserving Using Fully Homomorphic Encryption", *International Journal of Intelligent Engineering & Systems*, vol. 16, no. 1, pp. 277-289, 2023.