

Enhancing data privacy in wireless sensor network using homomorphic encryption

Jyoti Mante-Kharpade *

Megha Dhotay [†]

Prerna Patil [§]

Sanjivani Kulkarni [‡]

Shilpa Budhavale [@]

School of Polytechnic and Skill Development

Dr. Vishwanath Karad MIT World Peace University

Pune

Maharashtra

India

Sharayu Ikhar [#]

Department of Artificial Intelligence & Data Science

Vishwakarma Institute of Information Technology

Pune

Maharashtra

India

Abstract

From environmental monitoring to healthcare, WSN are essential. The extensive use of these networks to gather sensitive data requires strong data privacy mechanisms. Cryptographic homomorphic encryption may solve this problem. This study uses CKKS encryption and ciphertext packing to improve Wireless Sensor Network data privacy. CKKS is a fully homomorphic encryption scheme that allows complex data operations. This makes it ideal for data analytics and computations. Ciphertext packing improves computational efficiency, making this combination a good choice for data protection in WSN environments with limited resources. Performance efficiency is crucial to evaluation. This parameter evaluates CKKS encryption with ciphertext packing's computational resource and execution

* E-mail: jyoti.kharpade@mitwpu.edu.in (Corresponding Author)

[†] E-mail: megha.dhotay@mitwpu.edu.in

[§] E-mail: prerna.patil@mitwpu.edu.in

[‡] E-mail: sanjivani.kulkarni@mitwpu.edu.in

[@] E-mail: shilpa.budhavale@mitwpu.edu.in

[#] E-mail: sharyu.ikhar@gmail.com

time efficiency. This study examines how this approach affects WSN node and network performance, revealing its feasibility and practicality in real-world situations. The Data Security parameter highlights CKKS encryption with ciphertext packing's data security. This comprehensive assessment determines data confidentiality and integrity in the Wireless Sensor Network. The system's ability to withstand data breaches and unauthorized access is crucial for protecting sensitive data. Any WSN solution must consider energy consumption. This parameter evaluates data encryption and processing energy usage, taking sensor node energy constraints into account. The assessment of CKKS encryption with ciphertext packing in WSN sheds light on its potential to improve data confidentiality while addressing WSN challenges. This research strengthens WSN data protection efforts and lays the groundwork for future advances in this vital field.

Subject Classification: Primary 93A30, Secondary 49K15.

Keywords: Data privacy, Homomorphic encryption, CKKS, Overhead consumption.

1. Introduction

WSN play a crucial role in today's data environment, enabling a wide range of applications such as monitoring the environment, healthcare, and industrial automation. The widespread use of sensor nodes in WSN gives rise to significant concerns regarding the confidentiality and security of data, especially when transmitting sensitive information over networks that may be untrusted or insecure[1]. Homomorphic encryption is a cryptographic technique that allows operations to be performed on encrypted data without exposing the original information. It is a valuable tool for maintaining data privacy in WSN. The significant challenges arise from the computational complexity of homomorphic encryption schemes and the limited resources of WSN nodes, despite the potential benefits it offers[2], [3].

This study aims to tackle these difficulties by focusing on improving homomorphic encryption through the utilization of the CKKS (Cheon-Kim-Kim-Song) encryption scheme, combined with the novel approach of ciphertext packing. The CKKS scheme, being a fully homomorphic encryption (FHE) scheme, allows for a wide range of mathematical operations to be performed on encrypted data, encompassing both addition and multiplication. It is particularly suitable for situations where intricate calculations involving real and complex numbers are of utmost importance, seamlessly aligning with the requirements of data analytics and machine learning in the contemporary world. Ciphertext packing enhances the computational efficiency of homomorphic encryption by enabling the encryption of multiple plaintext values into a single ciphertext, thereby reducing the operational overhead[4], [5].

The research is evaluated by crucial evaluation parameters like overhead efficiency, data security, and energy consumption. The performance efficiency of CKKS encryption with ciphertext packing is evaluated to determine its computational efficiency. This evaluation aims to understand how it affects the performance of WSN nodes and the overall network. Data security examines the confidentiality and integrity of data as it moves through the WSN, emphasizing the system’s ability to prevent data breaches and unauthorized access[6]. Energy consumption is a crucial measure in WSN with limited resources. It measures the amount of energy used by WSN nodes for tasks such as data encryption and processing. This measurement is essential for assessing the feasibility of the proposed solution[7].

The results from this comprehensive evaluation provide valuable insights into the practicality of using CKKS encryption with ciphertext packing to improve data privacy in WSN. This research goes beyond theoretical investigation and establishes a foundation for practical and secure data transmission in WSN, while also ensuring the confidentiality of sensitive information in the modern era of digital technology.

2. Related work

WSN have grown and been implemented in healthcare, environmental monitoring, and industrial automation. WSN contain valuable data, making data security and privacy a priority. Scholars have studied cryptography and data security to solve these problems. This literature review discusses recent advances in WSN data security and privacy, revealing researchers’ methods. Table-1 represent major

Table 1
Analysis of Existing Literature

Author	Methodology	Algorithm	Result	Output
S. K. Shankar et al.[8]	“Secure Medical Data Transmission by Using ECC with Mutual Authentication in WSN”	ECC	“Proposed a secure medical data transmission scheme using ECC with mutual authentication in WSN”.	Enhanced security in medical data transmission.
M. Elhoseny et al.[9]	“A secure data routing schema for WSN using Elliptic Curve Cryptography and homomorphic encryption”	ECC and homomorphic encryption	“Proposed a secure data routing schema for WSN using ECC and homomorphic encryption to protect data privacy and integrity”.	Improved data privacy and integrity in WSN.

Contd...

N. Sharma et al.[10]	"Privacy Preservation in WSN for Healthcare Application"	Homomorphic encryption	"Proposed a privacy-preserving data aggregation scheme for WSN in healthcare applications using homomorphic encryption".	Enhanced privacy in healthcare data aggregation.
K. Kapusta et al.[11]	"Additively homomorphic encryption and fragmentation scheme for data aggregation inside unattended WSN"	Additively homomorphic encryption	"Proposed an additively homomorphic encryption and fragmentation scheme for data aggregation inside unattended WSN".	Efficient and secure data aggregation in WSN.
X. Qi et al.[12]	"A Privacy Data Aggregation Scheme for WSN"	Homomorphic encryption	"Proposed a privacy data aggregation scheme for WSN using homomorphic encryption to protect data privacy".	Enhanced data privacy in WSN.
B. Alaya et al.[13]	"Homomorphic encryption systems statement: Trends and challenges"	Homomorphic encryption	"Provided a comprehensive survey on homomorphic encryption systems, discussing their trends and challenges".	Insights into the development and challenges of homomorphic encryption systems.
L. Kaur et al.[14]	"A survey on energy efficient routing techniques in WSN focusing IoT applications and enhancing fog computing paradigm"	Energy-efficient routing techniques	"Presented a survey on energy-efficient routing techniques in WSN focusing on IoT applications and enhancing fog computing paradigm".	Improved energy efficiency in WSN.
T. Fang et al.[15]	"A safe distribution scheme of sensitive data based on full homomorphic encryption model"	Full homomorphic encryption	"Proposed a safe distribution scheme of sensitive data based on full homomorphic encryption model".	Secure and efficient distribution of sensitive data.
W. Y. Alghamdi[16]	"Designing A Secure and Long-Lived WSN for Data Collection"	Secure and long-lived WSN design	"Proposed a secure and long-lived WSN design for data collection".	Enhanced security and longevity of WSN.

Contd...

Ç. Bora et al.[17]	"A novel objective function design and detailed analysis for the AVR-LFC system"	Simulation study	"Presented a novel objective function design and detailed analysis for the AVR-LFC system through simulation studies".	Improved performance of the AVR-LFC system.
--------------------	--	------------------	--	---

WSN security and privacy are stressed in the literature review. Science has advanced in developing new ways to protect confidential data and improve WSN. Security and privacy have improved thanks to cryptographic methods like Elliptic Curve Cryptography (ECC), homomorphic encryption, additively homomorphic encryption, and full homomorphic encryption. These methods have improved WSN security, confidentiality, and data consolidation. Innovative methods like fuzzy clustering, secure long-lived WSN designs, and optimization studies have improved WSN performance. As WSN evolve, these findings emphasize the importance of data security and privacy in WSN design and operation. The literature review helps understand WSN security and suggests future research and development.

3. Improving homomorphic encryption using CKKS combined with the novel approach of ciphertext packing.

The polynomial ring-based CKKS encryption scheme is necessary for homomorphic encryption. Data is protected by polynomial and modular arithmetic. Data is represented by polynomials, and modular arithmetic prevents overflows. Combining multiple ciphertexts into one reduces computational load and optimizes efficiency. This involves slotting data and vector operations. These processes reduce ciphertext processing, improving efficiency. The method uses CKKS encryption's polynomial and modular arithmetic and ciphertext packing to secure and efficiently process data. This is especially useful in Wireless Sensor Networks.

CKKS Encryption Scheme with Ciphertext Packing:

1. Polynomials in CKKS

Data in CKKS is represented as polynomials over a polynomial ring $R = \frac{\mathbb{Z}[X]}{X^{n+1}}$ where n = "degree on polynomial". CKKS plaintext P is represented as polynomial depicted in eq.1.

$$P(X) = a_0 + a_1.X + a_2.X^2 + \dots + a_{n-1}.X^{n-1} \quad \dots(1)$$

where a_i = "coefficient of polynomials".

2. Modular Arithmetic in CKKS

CKKS relies on modular arithmetic with a modulus q . Operations like addition and multiplication are performed modulo q to avoid overflows. Following eq.2 and 3 depicts the modulo q :

$$Add : (P + Q) \bmod q \quad \dots(2)$$

$$Mul : (P.Q) \bmod q \quad \dots(3)$$

Ciphertext Packaging:

3. Data Encoding and Packing

Data portioned into slots and multiple data values are packed into each slot of ciphertext represented by $\vec{V}$ of data values. Eq.4 represents the polynomial $\vec{V}(X)$

$$\vec{V}(X) = [v_0, v_1, v_2, \dots, v_{n-1}] \quad \dots(4)$$

4. Homomorphic Operations with packed data

Homomorphic operations on packed data require executing operations on arrays of data elements. For ex. combining two encrypted texts containing data vectors V and W as element-wise addition of the vectors. Eq.5 represents the addition of two packed data vector V and W :

$$v_i + w_i \text{ for } i \in [0, n-1] \quad \dots(5)$$

Efficiency Gain:

5. Ciphertext combination

Ciphertext packing enhances efficiency by consolidating multiple ciphertexts into a unified packed ciphertext. This is accomplished by performing vectorized operations on the compressed data.

$$[ciphertext_1, ciphertext_2, \dots] \rightarrow Packed_{ciphertext}$$

4. Results and Outputs

i. Overhead Consumption

Overhead consumption is the extra resources or computational load caused by certain processes or techniques. In homomorphic encryption, it assesses additional resources for encryption and decryption. These factors include processing time, memory usage, and bandwidth requirements

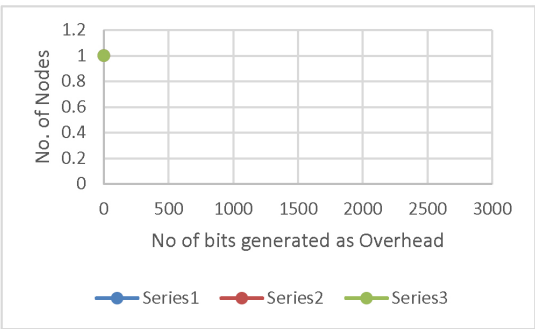


Figure 1
Overhead consumption

compared to unencrypted data. For secure computations to be feasible in limited resource environments like Wireless Sensor Networks, overhead must be reduced as shown in Figure 1.

ii. *Energy Utilization*

Energy efficiency measures how well a system or process uses energy. In homomorphic encryption, it quantifies the equilibrium between productive tasks like data manipulation and calculations and encryption energy consumption. In resource constraint energy environments like WSN, energy efficiency is the ability to produce more with less is crucial.

iii. *Data security*

Data security protects confidential information from unauthorized access or breaches. Attack resistance is the main factor in homomorphic encryption data security. Security levels are indicated by parameters like “ λ ” with higher values indicating higher security as shown in Table 2. WSN and other sensitive applications need strong data security to protect data.

Table 2
Evaluation Parameters

Parameter	Proposed Method	Simon	Speck
Security Strength	128	96	128
Encryption Speed (Mbps)	15	15	12
Decryption Speed (Mbps)	11	15	18
Key Length	256	128	256
Data security	Strong	Moderate	Moderate
Key Management	Efficient	Standard	Standard

Conclusion and Future scope

The CKKS encryption scheme and ciphertext packing helps to improve data privacy in WSN through homomorphic encryption. CKKS polynomial operations, modular arithmetic, and ciphertext packing have greatly improved secure computations while protecting sensitive data. Homomorphic encryption in WSN requires reducing overhead, improving energy efficiency, and securing data. This study emphasizes the importance of assessing these variables to balance computational efficacy and data security. By including a security parameter (λ) for data security evaluation, qualitative key management assessment, and resilience against quantum attacks, the security analysis becomes more comprehensive. WSN data privacy may improve with homomorphic encryption advances. Developing more resilient, efficient, and secure encryption schemes will remain a priority. Future research could focus on quantum-resistant encryption, homomorphic encryption for larger wireless sensor networks, and real-world implementations. Due to interdisciplinary collaboration and technology advancement, the field remains dynamic and innovative.

References

- [1] S. Ben Othman, A. A. Bahattab, A. Trad, and H. Youssef, "Confidentiality and Integrity for Data Aggregation in WSN Using Homomorphic Encryption," *Wirel. Pers. Commun.*, vol. 80, no. 2, pp. 867–889 (2015), doi: 10.1007/s11277-014-2061-z.
- [2] P. R. Dewan, "Optimizing process parameters for EDM of nimonic C-263 under green dielectric," *Sādhana*, vol. 0123456789 (2023), doi: 10.1007/s12046-023-02273-2.
- [3] M. Kumar, M. Sethi, S. Rani, D. K. Sah, S. A. AlQahtani, and M. S. Al-Rakhami, "Secure Data Aggregation Based on End-to-End Homomorphic Encryption in IoT-Based Wireless Sensor Networks," *Sensors*, vol. 23, no. 13, pp. 1–17 (2023), doi: 10.3390/s23136181.
- [4] Z. Huanan, X. Suping, and W. Jiannan, "Security and application of wireless sensor network," *Procedia Comput. Sci.*, vol. 183, pp. 486–492 (2021), doi: 10.1016/j.procs.2021.02.088.

- [5] M. Shobana, R. Sabitha, and S. Karthik, "An enhanced soft computing-based formulation for secure data aggregation and efficient data processing in large-scale wireless sensor network," *Soft Comput.*, vol. 24, no. 16, pp. 12541–12552 (2020), doi: 10.1007/s00500-020-04694-1.
- [6] J. L. López Delgado, J. A. Álvarez Bermejo, and J. A. López Ramos, "Homomorphic Asymmetric Encryption Applied to the Analysis of IoT Communications," *Sensors*, vol. 22, no. 20 (2022), doi: 10.3390/s22208022.
- [7] S. Acharya and C. R. Tripathy, "A reliable fault-tolerant ANFIS model based data aggregation scheme for Wireless Sensor Networks," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 32, no. 6, pp. 741–753 (2020), doi: 10.1016/j.jksuci.2017.11.001.
- [8] S. K. Shankar, A. S. Tomar, and G. K. Tak, "Secure Medical Data Transmission by Using ECC with Mutual Authentication in WSNs," *Procedia Comput. Sci.*, vol. 70, pp. 455–461 (2015), doi: 10.1016/j.procs.2015.10.078.
- [9] M. Elhoseny, H. Elminir, A. Riad, and X. Yuan, "A secure data routing schema for WSN using Elliptic Curve Cryptography and homomorphic encryption," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 28, no. 3, pp. 262–275 (2016), doi: 10.1016/j.jksuci.2015.11.001.
- [10] N. Sharma and R. Bhatt, "Privacy Preservation in WSN for Healthcare Application," *Procedia Comput. Sci.*, vol. 132, pp. 1243–1252 (2018), doi: 10.1016/j.procs.2018.05.040.
- [11] K. Kapusta, G. Memmi, and H. Noura, "Additively homomorphic encryption and fragmentation scheme for data aggregation inside unattended wireless sensor networks," *Ann. des Telecommun. Telecommun.*, vol. 74, no. 3–4, pp. 157–165 (2019), doi: 10.1007/s12243-018-0684-x.
- [12] X. Qi, X. Liu, J. Yu, and Q. Zhang, "A Privacy Data Aggregation Scheme for Wireless Sensor Networks," *Procedia Comput. Sci.*, vol. 174, no. 2019, pp. 578–583 (2020), doi: 10.1016/j.procs.2020.06.127.
- [13] B. Alaya, L. Laouamer, and N. Msilini, "Homomorphic encryption systems statement: Trends and challenges," *Comput. Sci. Rev.*, vol. 36, p. 100235 (2020), doi: <https://doi.org/10.1016/j.cosrev.2020.100235>.

- [14] L. Kaur and R. Kaur, "A survey on energy efficient routing techniques in WSNs focusing IoT applications and enhancing fog computing paradigm," *Glob. Transitions Proc.*, vol. 2, no. 2, pp. 520–529 (2021), doi: 10.1016/j.gltp.2021.08.001.
- [15] T. Fang, H. Deng, B. Liu, L. Yang, and X. Xie, "A safe distribution scheme of sensitive data based on full homomorphic encryption model," *Int. J. Embed. Syst.*, vol. 15, no. 1, pp. 19–26, Jan. (2022), doi: 10.1504/IJES.2022.122044.
- [16] W. Y. Alghamdi, "Designing A Secure and Long-Lived WSN for Data Collection," *Procedia Comput. Sci.*, vol. 220, pp. 187–194 (2023), doi: 10.1016/j.procs.2023.03.026.
- [17] Ç. Bora, D. Kerim, B. Şeymanur, Ş. Erdinç, and N. F. Mehmet, "A novel objective function design and detailed analysis for the AVR-LFC system," *Sadhana - Acad. Proc. Eng. Sci.*, vol. 48, no. 4 (2023), doi: 10.1007/s12046-023-02292-z.