iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** I **Month of publication:** January 2024

DOI: https://doi.org/10.22214/ijraset.2024.58180

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue I Jan 2024- Available at www.ijraset.com

Advancing Wireless Sensor Network Security through the Implementation of Homomorphic Encryption for Secure and Private Image Processing

Imam Adam Idris[1], Fadilul-lah Yassaanah issahku[2]
Anhui university of Science and Technology, School of Computer Science and Engineering, Huainan 232001, China

Abstract: ***Data security and privacy in image processing are of utmost concern. This paper presents an innovative architecture for integrating Homomorphic Encryption (HE) in Wireless Sensor Networks (WSNs), focusing on enhancing data security and privacy in image processing. Central to this architecture are sensor nodes equipped with Paillier Homomorphic Encryption capabilities, ensuring data confidentiality from the collection point. The network features intermediate aggregator nodes that perform homomorphic computations, such as summing or averaging, on encrypted data, maintaining its confidentiality. The central server, equipped with the private key, decrypts the aggregated data and is pivotal for complex data analyses, ensuring secrecy until the final stage. This architecture, characterized by the implementation of Homomorphic Encryption, allows for secure data encryption at the sensor nodes and its subsequent processing in an encrypted form. The design is bolstered by a robust mathematical framework, enhancing the system's security and effectiveness. This approach secures data within WSNs and harnesses the advanced capabilities of Homomorphic Encryption for data privacy and safety throughout the network's lifecycle.***

Keywords: ***Wireless Sensor Networks, Homomorphic Encryption, Data Security, Data Privacy, Image Processing, Sensor Nodes, Paillier Encryption.***

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have emerged as a pivotal technology for various applications, ranging from environmental monitoring to industrial automation. These networks consist of spatially distributed autonomous sensors that cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion, or pollutants. They also pass their data through the network to a central location.

The importance of WSNs in data collection and transmission cannot be overstated. They offer a unique blend of flexibility, cost-effectiveness, and ease of deployment, making them ideal for dynamic environments and applications where traditional wired networks are impractical or too expensive.

Recent advancements in WSNs focus on enhancing their efficiency and effectiveness. Chen and Tang (2022) introduced an energy-saving framework for heterogeneous WSNs, utilizing Unmanned Aerial Vehicles (UAVs) to assist in data collection. Their approach dynamically adjusts the working mode of sensor nodes based on their residual energy, optimizing energy thresholds and cluster head selection to minimize energy consumption while ensuring successful data transmission and adhering to UAV trajectory constraints [1].

Similarly, Jiao et al. proposed a novel data collection policy in wireless rechargeable sensor networks. Their strategy involves using a mobile vehicle as a data collector and an energy replenisher. This dual role of the mobile vehicle helps minimize energy consumption and improve data transmission performance, thereby enhancing the overall efficiency of the network [2].

Addressing the challenges of limited energy and unbalanced energy consumption in mobile wireless sensor networks, Yue et al. (2022) developed a path optimization mechanism based on an improved dragonfly optimization algorithm. This method minimizes energy consumption and improves reliability under time-delay constraints, enhancing the network's service quality and reliability [3].

Furthermore, Bilal, Munir, and Alarfaj (2022) contributed to this field by proposing a hybrid clustering and routing algorithm for heterogeneous WSNs.

Their model, which includes threshold-based data collection, aims to reduce unnecessary data transmissions and extend network stability in dense areas [4]. This approach has shown significant improvements in load balancing and end-to-end delay compared to other energy-efficient protocols.

WSNs play a crucial role in modern data collection and transmission, with ongoing research focusing on optimizing their energy efficiency, reliability, and overall performance. These networks are integral to advancing various sectors, including environmental monitoring, healthcare, and industrial automation.

The increasing deployment of Wireless Sensor Networks (WSNs) in sensitive domains such as surveillance, military operations, healthcare, and environmental monitoring underscores the critical need for secure image processing. In these applications, WSNs capture and transmit images, often containing sensitive information, necessitating stringent security measures during processing and transmission [5].

The primary concern in secure image processing within WSNs is safeguarding privacy and confidentiality. Particularly in healthcare and surveillance, the images captured by sensor nodes may contain private information. Protecting this data from unauthorized access is essential to maintain individual privacy and the confidentiality of sensitive information. Furthermore, the integrity of image data is crucial, especially in applications like military surveillance or environmental monitoring, where the authenticity and accuracy of data are paramount. Secure image processing mechanisms play a vital role in ensuring data integrity preventing tampering and alteration of the data [6].

Another critical aspect of secure image processing in WSNs is protecting against cyber attacks, including interception, tampering, and spoofing. Implementing robust encryption and other security measures is vital to shield the network from these threats, ensuring the secure transmission of images from sensor nodes to the base station. Moreover, compliance with stringent data security regulations in various industries necessitates the adoption of secure image processing practices in WSNs [7].

However, implementing effective security measures in WSNs faces challenges due to sensor nodes' limited computational power and energy resources. Given the potentially large number of sensor nodes in WSNs, the need for scalable security solutions is also pronounced. Additionally, the complexity of designing efficient and effective security protocols, considering the diverse applications and environments of WSNs, adds to the challenge. Balancing high-level security with network performance, particularly regarding speed and energy efficiency, is a significant concern. This balance is crucial, given the sensitive nature of the data handled by these networks and their varied applications [6], [8].

Homomorphic encryption is emerging as a transformative approach in data security, particularly within Wireless Sensor Networks (WSNs). This advanced cryptographic technique allows for computations on encrypted data without decryption, offering substantial benefits in terms of security and privacy within WSNs [9].

In WSNs, where sensor nodes collect and transmit potentially sensitive data, traditional encryption methods necessitate decryption for data processing or analysis, posing significant security risks. Homomorphic encryption addresses this by enabling data processing in its encrypted form, thus maintaining data confidentiality even during analysis [10].

Integrating homomorphic encryption into WSNs enhances data security by keeping the data encrypted throughout its journey, significantly reducing the risks associated with data breaches and eavesdropping. This is particularly crucial in applications involving personal data, such as healthcare monitoring systems, or in scenarios demanding high confidentiality, like military surveillance [11].

Moreover, homomorphic encryption contributes to the preservation of privacy in WSNs. It allows for the aggregation and analysis of data without exposing the actual data content, which is especially relevant in scenarios where WSNs collect personal or sensitive information. User privacy is upheld by ensuring the data remains encrypted [12].

However, the implementation of homomorphic encryption in WSNs faces challenges, mainly due to the computational complexity associated with this form of encryption, which might strain the limited computational resources of sensor nodes. Balancing the security benefits with the computational overhead is a crucial area of ongoing research in applying homomorphic encryption in WSNs [9].

Integrating homomorphic encryption into Wireless Sensor Networks offers a promising pathway to enhance data security and privacy, potentially improving network efficiency. As this technology continues to evolve, its application in WSNs could become a cornerstone in pursuing more secure and efficient wireless sensor networks.

The primary objective of our paper is to explore and establish the efficacy of homomorphic encryption to enhance security and privacy in Wireless Sensor Networks (WSNs), particularly in the context of image processing.

This research addresses the dual challenges of maintaining data confidentiality and ensuring the integrity of image data transmitted across WSNs.

The specific objectives of the paper are:

1) To investigate the application of homomorphic encryption in WSNs, thus, the theoretical and practical aspects of implementing homomorphic encryption in WSNs, assessing its feasibility and performance in real-world scenarios.

2) To demonstrate the effectiveness of homomorphic encryption for image data through experimental analysis and simulations to showcase how homomorphic encryption can securely handle image data in WSNs without compromising data privacy.

Main contributions

a) Provides a detailed analysis of the security challenges in WSNs, mainly focusing on the vulnerabilities in image data transmission and processing.

b) Introduces a novel approach to employing homomorphic encryption in WSNs for image processing, contributing to the body of knowledge in cryptographic applications in sensor networks.

c) By implementing homomorphic encryption, the paper demonstrates a significant enhancement in the privacy and security of image data in WSNs, addressing a critical gap in current security protocols.

II. LITERATURE REVIEW

Integrating Homomorphic Encryption (HE) into Wireless Sensor Networks (WSNs), several studies have laid the groundwork, each contributing unique perspectives and methodologies. Raju Ranjan and Vinay Kumar Ahlawat explored using the Paillier homomorphic cryptosystem in WSNs, focusing on encrypting individual transmissions from sensor nodes and employing a digital signature method for authentication [13]. While emphasizing data security, their approach does not delve into the distributed processing of encrypted data across the network.

Mukesh Kumar et al. presented an End-to-End Homomorphic Encryption (EEHE) system for IoT-based WSNs, concentrating on secure data aggregation and the application of aggregator functions on encrypted messages [14]. This study shares a conceptual similarity with our proposed methodology regarding using HE for secure data aggregation. However, the architectural specifics differ, particularly in the roles assigned to various network components and the emphasis on scalability and computational distribution.

In a more specialized context, Usha et al. developed a Secure Cross-Layer Routing Protocol (SCLRP) for Underwater Acoustic Sensor Networks (UASNs) using homomorphic encryption combined with fuzzy logic [15] to target a specific type of WSN and incorporates fuzzy logic, which is not a feature of our proposed system architecture.

Hong et al. explored homomorphic encryption with Elliptic Curve Cryptography (ECC) to enhance mobile wireless network security and minimize communication overhead. While focusing on network security, their protocol presents a different application of HE and does not explicitly address the unique challenges of WSNs in distributed data processing [16].

Despite these significant contributions, there remains a research gap in the application of HE in WSNs, particularly in developing a system architecture that efficiently balances security, computational overhead, and scalability. Our proposed methodology addresses this gap by introducing a novel system architecture with sensor nodes equipped with data encryption capabilities, intermediate aggregator nodes performing homomorphic computations, and a central server for complex computations and data decryption. This architecture is designed to distribute the computational load effectively across the network, thereby enhancing the efficiency and scalability of the WSN while maintaining robust data security and privacy.

By focusing on a distributed approach to processing encrypted data, our methodology offers a comprehensive solution adaptable to various WSN scenarios, unlike the more specialized or limited-focus approaches in the existing literature. The integration of HE in this manner presents a promising avenue for advancing the security and functionality of WSNs, paving the way for more secure, efficient, and scalable sensor network applications.

Top of Form

III. BACKGROUND

A. Homomorphic Encryption: Principles and Applications

Homomorphic encryption is a form of encryption that allows computations to be performed on ciphertexts, generating an encrypted result that, when decrypted, matches the result of operations performed on the plaintext. This property makes it a powerful tool for secure data processing in environments where confidentiality is paramount, such as in Wireless Sensor Networks (WSNs).

The mathematical underpinnings of homomorphic encryption are rooted in number theory and algebra. We need to delve into some key concepts and equations to understand them.

1) Basic Concepts

- *Plaintext and Ciphertext:* In any encryption scheme, the original data is referred to as the plaintext, while the encrypted data is known as the ciphertext. Homomorphic encryption schemes transform plaintext into ciphertext so that specific types of operations yield encrypted results corresponding to the desired operations on plaintexts.
- *Encryption and Decryption Functions:* Let E denote the encryption function and D the decryption function. For a plaintext m and a key k, the encryption is represented as $E_{k(m)}$, and the decryption of a ciphertext c is $D_{k(c)}$.

2) Homomorphic Properties

- *Additive Homomorphism:* An encryption scheme is additively homomorphic if $E_{k(m_1)} + E_{k(m_2)} = E_{k(m_1+m_2)}$. This means that adding two encrypted numbers and then decrypting the result is the same as adding the two original numbers.
- *Multiplicative Homomorphism:* A scheme is multiplicatively homomorphic if $E_{k(m_1)} \times E_{k(m_2)} = E_{k(m_1 \times m_2)}$. Here, multiplying two ciphertexts and then decrypting yields the same result as multiplying the original plaintexts.

3) Example Schemes

- *RSA Encryption:* RSA is inherently multiplicatively homomorphic. Given two ciphertexts $c_1 = E_{k(m_1)and}\, c_2 = E_{k(m_2)}$, their product $c_1 \times c_2$ will decrypt to $m_1 \times m_2$.
- *Paillier Cryptosystem:* This is an example of an additively homomorphic encryption scheme. In Paillier, the sum of two ciphertexts will decrypt to the sum of their corresponding plaintexts.

For an additively homomorphic encryption scheme like Paillier, the encryption of a message m with a public key pk can be represented as:

$$E_{pk(m)} = g^m \times r^n mod\ n^2$$

Where g and n are part of the public key and r is a random number. The decryption with a private key sk involves a more complex process based on the modular multiplicative inverse.

Homomorphic Encryption (HE) is a form of encryption that allows computations to be performed on encrypted data, generating an encrypted result that, when decrypted, corresponds to the result of operations performed on the plaintext. HE can be categorized into three types based on the extent of operations it supports: Partially Homomorphic Encryption (PHE), Somewhat Homomorphic Encryption (SHE), and Fully Homomorphic Encryption (FHE).

B. Types of Homomorphic Encryption

1) Partially Homomorphic Encryption (PHE)

PHE supports either addition or multiplication, but not both. It allows an unlimited number of operations but only of one type. For example, the RSA encryption algorithm is a classic example of PHE with multiplicative properties. In RSA, the product of two ciphertexts decrypts to the product of their corresponding plaintexts.

2) Somewhat Homomorphic Encryption (SHE)

SHE supports a limited number of both addition and multiplication operations. The limitation is due to the growth of noise in the ciphertext, eventually making it undecryptable if too many operations are performed. For instance, the DGHV (van Dijk, Gentry, Halevi, and Vaikuntanathan) scheme is an example of SHE. It allows limited additions and multiplications before the noise becomes too great.

3) Fully Homomorphic Encryption (FHE)

FHE supports an unlimited number of both addition and multiplication operations on ciphertexts. It is the most versatile form of HE and is computationally intensive.

Gentry's FHE scheme, based on lattice-based cryptography, is a well-known example. It includes a "bootstrapping" process that reduces ciphertext noise, allowing unlimited operations.

Homomorphic Encryption (HE) has found its applications across various domains, each leveraging its ability to perform computations on encrypted data, thus ensuring data privacy and security.

In the realm of cloud computing, HE is a game-changer. It allows users to encrypt their data before uploading it to cloud services. The revolutionary aspect of this approach is that cloud providers can compute on this encrypted data without ever needing to access

the plaintext. This capability ensures the privacy and security of user data, a critical concern in today's digital age, where data breaches are increasingly common.

Additionally, it enables the secure aggregation and analysis of patient data for research purposes while maintaining strict confidentiality. Researchers, for instance, can perform statistical analyses on encrypted medical records. This method allows them to identify health trends or assess the efficacy of drugs without ever accessing sensitive patient information directly. Such an approach is invaluable in research areas where patient privacy is paramount.

Furthermore, HE offers a robust solution for secure data sharing and analysis. Banks and other financial institutions can utilize HE to perform encrypted searches on customer data. This application is particularly useful in fraud detection, where sensitive customer information needs to be analyzed without compromising individual privacy. By using HE, banks can ensure the confidentiality of customer data while still harnessing it for essential analytical purposes.

Moreover, in e-voting systems, HE can be used to ensure that votes are counted accurately while preserving voter anonymity. Voters can encrypt their votes, which can be tallied homomorphically, producing an encrypted result. Only authorized parties can decrypt the final count, ensuring the integrity of the voting process while maintaining the confidentiality of individual votes.

Finally, HE secures data aggregation, especially in IoT devices, which often collect sensitive data and need to be processed without compromising the privacy of individual data sources. HE allows for the secure aggregation of this data from multiple devices. This application is particularly relevant in scenarios where sensitive information is collected across a diverse array of sources and requires processing that respects the confidentiality of each data point.

IV. METHODOLOGY: INTEGRATING HOMOMORPHIC ENCRYPTION IN WIRELESS SENSOR NETWORKS

A. *Proposed System Architecture*

The proposed architecture for integrating Homomorphic Encryption in Wireless Sensor Networks is a sophisticated system designed to enhance data security and privacy while maintaining efficient network operations. At its core, the architecture features sensor nodes responsible for data collection and primary processing. These nodes are uniquely equipped with encryption capabilities, enabling them to apply homomorphic encryption to data at the collection point and secure it from the outset.

For the key generation phase, HE respectively generates the confidential key ck and general key gk

As follows:

$$ck = \boldsymbol{s}$$
$$gk = (gk*, \boldsymbol{y})$$

The public key gk is then communicated by HE to the source nodes, enabling them to encrypt the plaintexts that they have detected. Choose a random number t from $(-2s', 2s'), m \in \{0,1\}$, and a random subset $S \subseteq \{1,2,\dots,\tau\}$.Next, after selecting the source data, each source sensor node uses pk to produce the following ciphertext:

$$\boldsymbol{c} \leftarrow [m + 2m + 2\,\boldsymbol{Lm}xi]$$
$$i \in m \quad x_0$$

In reference to the public key, sample $xi \leftarrow D\gamma, s(s)\ for\ i = 0,\dots,T$, where:
$D(p) =$ Fchoose $q \quad Z \cap [0,2\gamma/s), m \quad Z \cap (-2s, 2s)$: output $x = sq + m\}$

Following that, this ciphertext (c) is sent to the aggregator or subsequent forwarding node for processing.

Integrity detection and data aggregation

Data can be directly aggregated by an aggregator for the HE scheme's property when the data is transferred to it. We only do addition and multiplication on the integers in our scheme. Using the (integer) addition and multiplication gates of $Z\varepsilon$, apply the (binary) circuit $Z\varepsilon$ with d inputs and b ciphertexts Zi. Perform all operations over the integers, and return the resultant integer $c*$, which satisfies Decrypt~~m~~sk, $Z*) = Z(m2,\dots,mb)$:

$$Z* = \text{Assess}(Zk, Z, c1, \dots, Zb)$$

Upon producing the ciphertext $Z*, then\ for\ i \in \{2,\dots,Q\}$, set

$$i \leftarrow [c* \cdot Bi]2$$

We present a data aggregation and integrity detection algorithm to test the data integrity and detect any fake data injections across the entire network, hence achieving data secrecy, data integrity, and false data detection during data aggregation and data forwarding.

Decrypting Data, The following equation yields the final answer when the data arrive at BS. We can determine that the outcome can be accurately decrypted from:

$$m' \leftarrow [Z * -l\sum_i sizil]$$

As the data moves through the network, it encounters intermediate aggregator nodes. These nodes are strategically placed to perform homomorphic computations on the encrypted data received from the sensor nodes. This capability allows them to perform specific calculations, such as summing or averaging, directly on the encrypted data, thus preserving its confidentiality.

The central server in this architecture plays a pivotal role. Unlike the sensor and aggregator nodes, the central server is a more powerful computing system capable of handling complex computations. It is the only point in the network where decryption of the aggregated data occurs, allowing for further analysis or computations on the decrypted data.

The secure communication links connecting the sensor, aggregator, and central servers are integral to the architecture. These links are crucial for the safe transmission of encrypted data and computational results throughout the network, ensuring that the integrity and confidentiality of data are maintained at all times.

The implementation of Homomorphic Encryption is a key aspect of this architecture. At the sensor nodes, data is encrypted using a public key before it is transmitted. The intermediate nodes then leverage the homomorphic properties of this encryption to perform operations on the encrypted data. The culmination of this process occurs at the central server, where the data, equipped with the private key, is finally decrypted for subsequent analysis.

A robust mathematical framework governing encryption and decryption processes is underpinning this entire architecture. The encryption function at the sensor nodes and the homomorphic properties utilized at the aggregator nodes are based on specific mathematical formulations. These formulations are critical to ensuring the security and practicality of operations on encrypted data within the network.

This architecture provides a secure and efficient method for handling data in Wireless Sensor Networks. It leverages the advanced capabilities of Homomorphic Encryption to ensure data privacy and security throughout the network's operation.

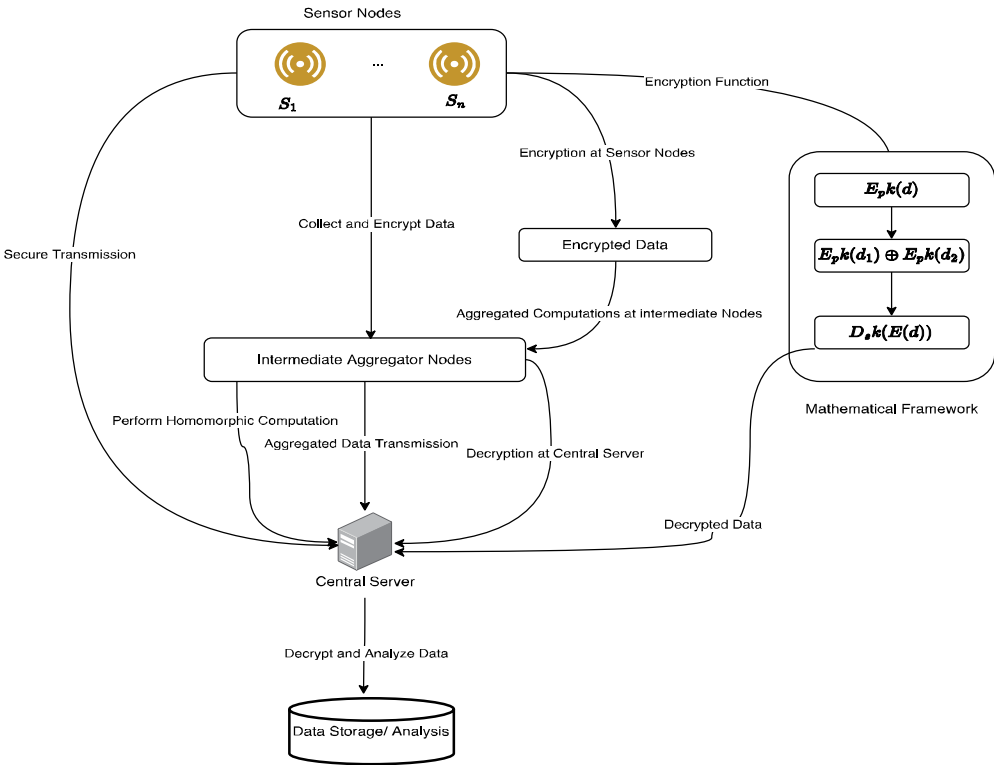


Figure 1. System Architecture for Homomorphic Encryption Integration in Wireless Sensor Networks

B. Homomorphic Encryption Implementation

Encryption of a Sensor Node:

In the proposed system architecture for integrating Homomorphic Encryption (HE) in Wireless Sensor Networks (WSNs), the encryption process at the sensor nodes is a crucial component. This process is foundational to ensuring the security and privacy of the data as it moves through the network.

Each sensor node in the network is configured with a public key, pk, which is part of the HE scheme for encrypting data before it is transmitted across the network. The public key is securely distributed to the sensor nodes during the network setup phase. The sensor nodes collect data from their environment, such as temperature readings, images, sound recordings, etc. Let's denote a piece of collected data as d.

Once the data d is collected, the sensor node encrypts it using the public key pk. The encryption process transforms the plaintext data d into an encrypted form, $E_{pk}(d)$, ensuring that the data's confidentiality is maintained.

The encryption function is mathematically represented as follows: $E_{pk(d)} = g^d \cdot r^n mod\ n^2$ Where g and n are the public key pk components, and r is a random number chosen for each encryption process. This formula is indicative of an encryption scheme like the Paillier cryptosystem, which is additively homomorphic.

The encrypted data, $E_{pk}(d)$, is then transmitted through the network to either an intermediate aggregator node or directly to the central server, depending on the network's configuration. During transmission, the encrypted data remains secure, as only the entity with the corresponding private key can decrypt and access the original data d.

The encrypted data retains the homomorphic properties of the encryption scheme. This means that certain types of computations can be performed directly on the encrypted data, $E_{pk}(d)$, without needing to decrypt it first.

Data encryption at the sensor nodes is a critical step in securing WSNs. By ensuring that data is encrypted right at the point of collection, the system significantly reduces the risk of data being intercepted and compromised, essential in scenarios where the sensor nodes are deployed in unsecured or public spaces.

Moreover, using a homomorphic encryption scheme allows for aggregating and analyzing encrypted data, a powerful tool for preserving privacy while still extracting meaningful insights from the collected data. This capability is particularly beneficial in applications where data confidentiality is as crucial as data analysis, such as healthcare monitoring or environmental data analysis.

C. Aggregated Computations At Intermediate Nodes

In the proposed system architecture for integrating Homomorphic Encryption (HE) in Wireless Sensor Networks (WSNs), the role of intermediate nodes is pivotal for aggregated computations. These nodes act as crucial junctions where data from multiple sensor nodes converge and are processed in an encrypted form.

Intermediate nodes are strategically positioned within the network to receive encrypted data transmitted efficiently by multiple sensor nodes. Each piece of this data is represented as $E_{pk}(d_i)$ where d_i is the data from the i^{th} sensor node is encrypted using the same public key pk. The core functionality of these intermediate nodes is to perform homomorphic operations on the received encrypted data. We employ sum functions for the data points,

If the intermediate node receives encrypted data points $E_{pk}(d_1), E_{pk}(d_2), \dots, E_{pk}(d_n)$, We compute the sum of these encrypted values directly. The operation is represented as:

$$E_{pk}(d_1) + E_{pk}(d_2) + \cdots + E_{pk}(d_n)$$

This operation leverages the additive homomorphic property of the encryption scheme, which allows the summation of encrypted data to yield the encrypted sum of the original data.

A significant advantage of this process is that these computations are performed without ever decrypting the data. This means the intermediate nodes do not need access to the private key, and the data remains secure and private throughout this processing stage. The ability to compute encrypted data ensures that sensitive information remains confidential, a crucial aspect in many applications of WSNs, such as in monitoring environments where data privacy is paramount.

The role of intermediate nodes in performing aggregated computations on encrypted data addresses several challenges in WSNs. Firstly, it reduces the amount of data that needs to be transmitted to the central server, thereby conserving network bandwidth and energy resources. Secondly, it maintains the privacy and security of the data, as the intermediate nodes do not decrypt the data but still perform meaningful computations.

This approach is particularly beneficial when the network must aggregate data from various sensors to derive meaningful insights or make decisions based on collective data, such as in environmental monitoring or innovative city applications. By processing data in its encrypted form, the network ensures that individual data points remain confidential, and only the aggregated result, once decrypted at the central server, reveals the collective information.

D. Decryption And Final Computation At Central Server

The central server plays a critical role in the final data processing stage in the proposed architecture for integrating Homomorphic Encryption (HE) in Wireless Sensor Networks (WSNs). This stage involves decrypting aggregated encrypted data and subsequent computations or analyses. Here's an in-depth look at this process:

The central server, positioned as the ultimate recipient in the network architecture, receives the aggregated encrypted data from the intermediate nodes. This data represents the collective information processed homomorphically by the intermediate nodes, encapsulating inputs from multiple sensor nodes across the network.

Unlike the intermediate nodes, the central server possesses the private key to decrypt the received data. This private key is securely stored and managed on the server, ensuring only authorized personnel or systems can access it. Upon receiving the encrypted aggregated data, the central server applies the decryption function using its private key. The decryption process converts the encrypted aggregated result to its original, readable form. The decryption function$D_{sk}(E(d))$is applied at the central server, where sk is the private key. The decryption reveals the aggregated result of the original data.

Once the data is decrypted, the central server holds the aggregated result in plaintext form. This decrypted data is now available for further analysis or computations, which might be necessary for the network's intended application.

Depending on the network's objectives, these analyses can range from simple statistical evaluations to more complex data-processing tasks. For instance, in environmental monitoring applications, the server might analyze the aggregated data to detect patterns or anomalies in environmental parameters.

The decryption and final computation stage at the central server is a critical component of the proposed system architecture. It ensures that while the data remains secure and private throughout its journey in the network, it can still be utilized effectively for the intended purpose of the WSN. By centralizing the decryption process, the architecture ensures that sensitive data is only accessible at the most secure point in the network, thereby maintaining high levels of data security and privacy.

The ability to perform detailed analyses and computations on the decrypted data allows the network to extract meaningful insights from the aggregated information, making the system secure but also practical and helpful. The central server's role in performing final computations offers flexibility in how the data is used. Different types of analyses can be applied as needed, making the system adaptable to various applications.

E. Image Processing Operations On Encrypted Data

In the proposed methodology for integrating Homomorphic Encryption (HE) in Wireless Sensor Networks (WSNs), particularly for image processing operations, the system architecture allows certain types of computations to be performed directly on encrypted image data. This capability is crucial for maintaining data privacy while enabling meaningful image analysis. Here's a description of how image processing operations can be performed on encrypted data, following our methodology:

Consider an image captured by a sensor node, represented as a matrix of pixels, where each pixel value is denoted by p_{ij} for the pixel in the i^{th} row and j^{th} column. Each pixel value is encrypted using the public key pk of the homomorphic encryption scheme. The encrypted pixel value is represented as $E_{pk}(p_{ij})$. The encryption can be mathematically represented as:

$$E_{pk}(p_{ij}) = g^{p^{ij}} \cdot r^n mod\ n^2$$

Where g and n are part of the public key, and r is a random number chosen for each encryption process.

Intermediate nodes receive encrypted pixel values from multiple sensor nodes. Suppose an operation like averaging is required across multiple images. The intermediate node can compute the sum of encrypted pixel values for each corresponding pixel position across different images and then divide by the number of images. The sum of encrypted pixels $E_{pk(p_{ij})}$ for the same pixel position across k images can be represented as: $\sum_{m=1}^{k} E_{(pk)}(p_{ij}^{(m)})$

This sum is then divided by k for averaging, which can be performed after decryption at the central server due to the limitations in dividing encrypted values. The central server receives the aggregated encrypted data and decrypts it using the private key sk. The decryption of the aggregated sum for each pixel position can be represented as:

$$Dsk\left(\sum_{m=1}^{k} E_{pk}\left(p_{ij}^{(m)}\right)\right)$$

After decryption, the server computes the average for each pixel position by dividing the decrypted sum by the number of images k.

V. EXPERIMENTAL SETUP AND DATA COLLECTION

In our experimental setup, we explored the integration of Homomorphic Encryption within a Wireless Sensor Network (WSN) environment. The core of our software implementation was the Python Homomorphic Encryption (phe) library, which facilitated the Paillier Homomorphic Encryption scheme. This scheme is crucial for encrypting, decrypting, and performing computations on data while maintaining its encrypted state. We utilized Python and its libraries, such as PIL (Pillow) for image processing and numpy for handling numerical operations alongside the concurrent future module to enhance encryption performance through parallel processing. The matplotlib library was employed to visualize the original and processed images.

The hardware requirements for our experiment were not overly demanding, though we recommended using a multi-core processor to manage the computational load during the encryption phase efficiently.

Our network setup comprised a basic WSN with two sensor nodes labeled S_1 and S_2. Each node was equipped with an image sensor, capturing high-resolution images – a human image from S_1 and a dog image from S_2., representing common subjects in surveillance and monitoring systems. To maintain consistency and manage computational demands, we resized both images to $64 \; x \; 64$ pixels and converted them to grayscale.

The procedure began with each sensor node capturing an image. These images were then standardized by resizing and converting them to grayscale, preparing them for encryption using the Paillier Homomorphic Encryption scheme; every pixel of these images was encrypted at the respective sensor nodes, transforming each image into an array of encrypted numerical values as seen in Figure 2.

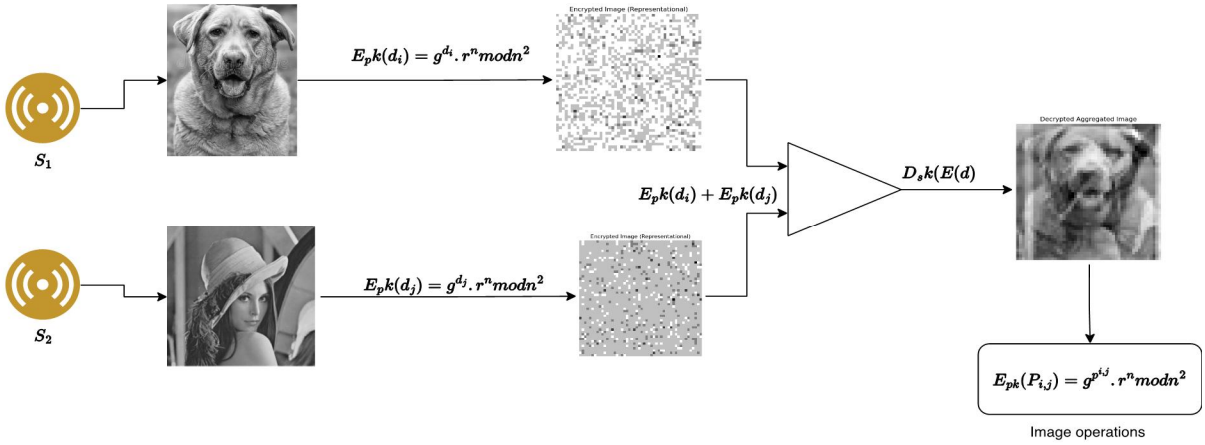


Figure 2. The encryption results.

The data was transmitted to an intermediate node within the network following encryption. This node performed a crucial step – the homomorphic aggregation of the encrypted pixel values from both images. This process, notably, did not involve decrypting the data, thus preserving the confidentiality of the information. Finally, the aggregated encrypted data was sent to the central server and decrypted to reveal the final processed image. This image represented the combined pixel values of the original human and dog images.

VI. RESULTS AND DISCUSSION

In our research, we delved into the integration of Homomorphic Encryption within Wireless Sensor Networks (WSNs), mainly focusing on image processing applications. Our findings present a nuanced view of this technology's capabilities and challenges.

The encryption process at the sensor nodes, owing to the Paillier Homomorphic Encryption scheme's computational complexity, was notably time-consuming. Encrypting each pixel individually contributed to extended processing times.

Similarly, the decryption phase at the central server involved substantial computation, especially given the need to handle aggregated data. Despite leveraging parallel processing techniques to mitigate the computational load, the overall process was still more demanding than conventional encryption methods.

The outcome of image processing after decrypting the aggregated data was particularly intriguing. The resultant image, a summation of pixel values from a human and a dog image, did not retain any meaningful visual content. However, it significantly demonstrated the ability to conduct computations on encrypted data, a pivotal aspect of Homomorphic Encryption.

Regarding security, the Paillier scheme provided robust protection, ensuring data privacy throughout transmission and processing. The encrypted data was secure from standard cryptographic attacks, rooted in the computational difficulty of solving complex mathematical problems, such as factoring large numbers. A standout feature of Homomorphic Encryption is its ability to process data while keeping it encrypted, thereby enhancing confidentiality.

Homomorphic Encryption stands out for its processing capabilities compared to traditional encryption methods. Unlike conventional methods that necessitate decryption before any data processing, Homomorphic Encryption allows for specific computations on encrypted data. While traditional encryption is generally faster and less resource-intensive, it lacks the capability for processing encrypted data. This distinction makes Homomorphic Encryption particularly valuable for sensitive WSN applications, where maintaining data privacy during processing is crucial.

Our experiment underscored the potential of Homomorphic Encryption in bolstering data security and privacy in WSNs. The capacity to process encrypted data without decryption is a considerable advantage in maintaining confidentiality, especially in sensitive environments. However, this comes at the cost of increased computational overhead, a trade-off that may be justified in scenarios where data privacy is paramount.

This technology holds particular promise in remote surveillance, environmental monitoring, and healthcare, where safeguarding data confidentiality is paramount. Our findings also highlight the necessity for continued research in this domain, focusing on optimizing Homomorphic Encryption techniques to reduce computational demands and develop more efficient algorithms suitable for WSNs.

A. Challenges and Limitations

Implementing Homomorphic Encryption (HE) in Wireless Sensor Networks (WSNs) presented notable challenges, primarily in computational complexity. Encrypting data, especially images, at the sensor nodes and performing homomorphic operations at intermediary points demanded substantial computational resources, leading to increased processing times. This complexity posed significant challenges in resource-constrained environments typical of WSNs. Additionally, the current study faced limitations in efficiently handling large volumes of data, a critical aspect for broader applicability in real-world scenarios. Future improvements could focus on optimizing encryption algorithms and developing more efficient processing techniques to reduce computational load. Enhancing the system's scalability to handle larger datasets with minimal resource expenditure remains crucial for further research and development.

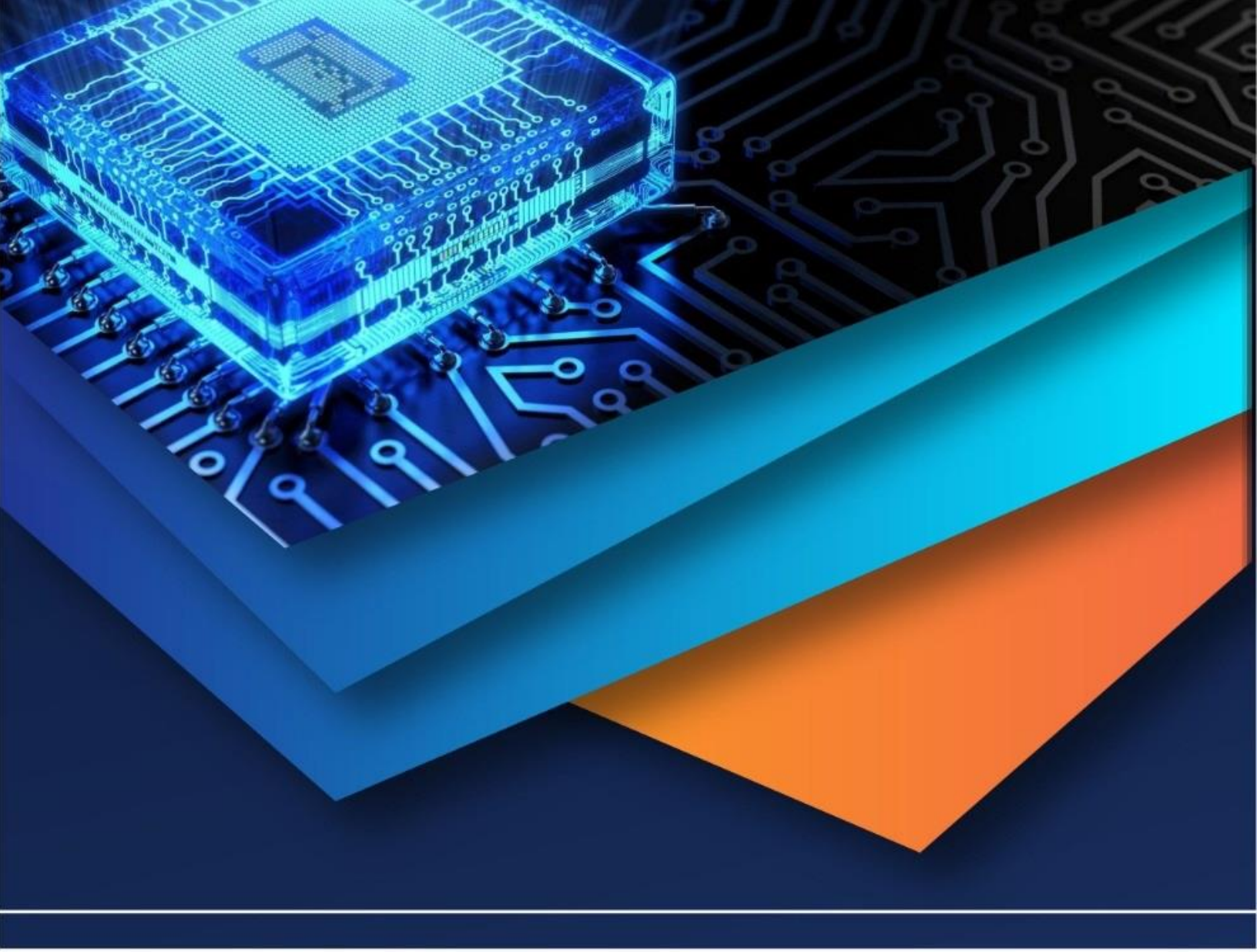
VII. CONCLUSION

Our study on integrating Homomorphic Encryption (HE) in Wireless Sensor Networks (WSNs) reveals significant advancements in securing network data, particularly in image processing applications. The HE implementation substantially enhances data security and privacy, mitigating risks associated with data transmission and processing within WSNs. This approach notably elevates the potential for secure image processing in such networks, enabling sensitive applications like surveillance and environmental monitoring to maintain data confidentiality. The implications of our findings are profound for WSN security, establishing a framework where data can be processed in encrypted form, thus preserving privacy without compromising the utility of the data. However, the challenges of computational complexity and resource constraints highlight the need for continued research. Future research should optimize encryption algorithms and processing methods to make HE more feasible for large-scale and real-world applications. Developing solutions that balance security, efficiency, and practicality will be crucial in advancing the field of secure data processing in WSNs.

REFERENCES

[1] J. Chen and J. Tang, "UAV-assisted data collection for dynamic and heterogeneous wireless sensor networks," IEEE Wireless Communications Letters, vol. 11, no. 6, pp. 1288–1292, 2022.
[2] W. Jiao, M. Tian, and Y. Xu, "A combining strategy of energy replenishment and data collection in wireless sensor networks," IEEE Sens J, vol. 22, no. 7, pp. 7411–7426, 2022.
[3] Y. Yue et al., "A data collection method for mobile wireless sensor networks based on improved dragonfly algorithm," Comput Intell Neurosci, vol. 2022, 2022.

[4] M. Bilal, E. U. Munir, and F. K. Alarfaj, "Hybrid clustering and routing algorithm with threshold-based data collection for heterogeneous wireless sensor networks," Sensors, vol. 22, no. 15, p. 5471, 2022.
[5] A. Z. Abualkishik, A. A. Alwan, and others, "Trust aware aquila optimizer based secure data transmission for information management in wireless sensor networks," Journal of Cybersecurity and Information Management, vol. 9, no. 1, pp. 40–51, 2022.
[6] M. S. Abood, H. Wang, H. F. Mahdi, M. M. Hamdi, and A. S. Abdullah, "Review on secure data aggregation in Wireless Sensor Networks," in IOP Conference Series: Materials Science and Engineering, 2021, p. 12053.
[7] L. Kocharla and B. Veeramallu, "Secure Energy-Efficient Load Balancing and Routing in Wireless Sensor Networks With Mediative Micro-ANN Fuzzy Logic," International Journal of Fuzzy System Applications (IJFSA), vol. 11, no. 3, pp. 1–16, 2022.
[8] M. Elhoseny, A. Farouk, J. Batle, A. Shehab, and A. E. Hassanien, "Secure image processing and transmission schema in cluster-based wireless sensor network," in Sensor Technology: Concepts, Methodologies, Tools, and Applications, IGI Global, 2020, pp. 698–715.
[9] S. V Phakade, C. R. Singla, and O. Rajankar, "Design of Privacy and Energy-Efficient DATA Aggregators for Wireless Sensor Networks," in 2022 2nd Asian Conference on Innovation in Technology (ASIANCON), 2022, pp. 1–5.
[10] H. Ma, Z. Zhang, H. Li, S. Yin, and C. Zhao, "A Provable Private Data Aggregation Scheme Based on Digital Signatures and Homomorphic Encryption for Wireless Sensor Networks.," J. Inf. Hiding Multim. Signal Process., vol. 8, no. 3, pp. 536–543, 2017.
[11] A. Singh, R. R. K. Chaudhary, and K. Chatterjee, "A novel privacy preservation mechanism for wireless medical sensor networks," in International Conference on Emerging Trends and Advances in Electrical Engineering and Renewable Energy, 2020, pp. 173–182.
[12] M. S. Huque and A. S. Kaurav, "A Novella Framework for Secure Data Aggregation in Wireless Sensor Networks using Symmetric Homomorphic Encryption Scheme (SHES)".
[13] J. Vijayan and G. Raju, "A New approach to Requirements Elicitation Using Paper Prototype," International Journal of Advanced Science and Technology, vol. 28, 2011.
[14] 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, 2023, doi: 10.3390/s23136181.
[15] M. Usha, R. Ashween, and others, "SCLRP-Architecture for Secure Cross-Layer Routing Protocol for Underwater Acoustic Sensor Networks using Fuzzy Logic and Enhanced Algebra Homomorphic Encryption," 2021.
[16] M. Hong, P.-Y. Wang, and W.-B. Zhao, "Homomorphic encryption scheme based on elliptic curve cryptography for privacy protection of cloud computing," in 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2016, pp. 152–157.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY