JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3806-3821
https://publishoa.com
ISSN: 1309-3452

A Sophisticated and Light weight Cryptographic Protocols for Data Security in Wireless Sensor Networks

[1]Dr. C. Srinivasa Kumar, [2]Dr. A.C. Priya Ranjani, [3]Dr. Pradeep Venuthurumilli, [4]Dr. A. Gautami Latha, [5]Dr. Ranga Swamy Sirisati

[1]Professor, Department of CSE, Vignan's Institute of Management and Technology for Women, Kondapur, Ghatkesar, Hyderabad, Telangana, EMail: drcskumar41@gmail.com

[2]Associate Professor, Dept. of CSE, Vijaya Institute of Technology for Women, Vijayawada, Andhra Pradesh, Mail: acpranjani@gmail.com

[3]Associate Professor, Department of CSE, ST.Mary's Women's Engineering College, Guntur, Andhra Pradesh, India-522017, Email: pradeepvenuthuru@gmail.com

[4]Professor, Department of CSE, Sridevi Women's Engineering College, Vattinagulapally, Hyderabad-500075, Telangana, India, E-Mail: gauthamilatha2021@gmail.com

[5]Associate Professor, Department of CSE, Vignan's Institute of Management and Technology for Women, Kondapur, Ghatkesar, Hyderabad , Telangana E-Mail: sirisatiranga@gmail.com

Received: 2022 March 15; **Revised:** 2022 April 20; **Accepted:** 2022 May 10

Abstract

Wireless Sensor Networks have been used practically every application because they give a cost-effective solution to real-world challenges. However, the sensor nodes have limited processing capacity, battery power, and memory. These nodes immediately transmit the measured environmental or physical data to the Base Station (BS). This direct transfer of data raises the cost of data connectivity. Furthermore, increased data exchange consumes more energy, reducing the lifespan of sensor networks. As a result, the data aggregation methodology is used in WSN to minimize transmission costs and extend the lifespan of sensor networks. Because the nodes are put in a hostile area and communicate through broadcast, the sensor nodes are quickly taken, and the aggregate data is quickly destroyed. As a result, data security is an important study topic in WSN. Because the sensor network has limited resources, specific wireless network security solutions cannot be used for WSN.The research that has been done indicates that lightweight block cyphers

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3806-3821
https://publishoa.com
ISSN: 1309-3452

are the most effective method for protecting health data. The Provably Secured Data Aggregation (PSDA) method evaluates the outcomes of the AES, Simon, and Speck lightweight cryptosystems. The Speck method involves less time for calculation, which means it can be used for encryption and decryption. As a direct consequence of this, the Speck algorithm is utilised in order to encrypt patient information.

Keywords: *Data Security, Wireless Sensor Networks, Data Aggregation, Energy Efficient.*

1 Introduction

Wireless Sensor Network (WSN) is now extensively employed in all industries, including the military, business, health, and academia. WSN is made up of many or thousands of sensor nodes that are physically distributed and linked to a base station to monitor environmental variables (BS). The sensor node detects the surroundings and sends data to the BS. Finally, the information is delivered from the BS to the users over the internet. The sensor network's qualities such as scalability, mobility, dependability, and responsiveness are why it is extensively used in various sectors. The sensor network design is shown in Figure 1.

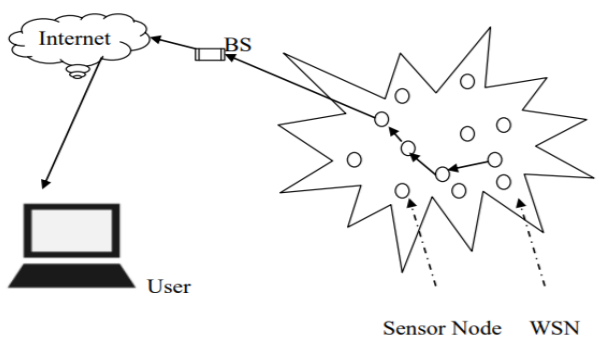

Figure 1: Architecture WSN

A sensor node is made up of four key components: a sensing unit, a processing unit, a communication module, and a power unit (Akyildiz et al. 2002) [2], and the sensing unit is made up of two subunits: sensors and an analog-to-digital converter (ADC). The ADC unit receives feedback from the sensors on variables like pressure, temperature, light, and humidity. The analogue signals that are generated by the sensors are sent into an ADC unit, which then converts them into digital signals. The processing unit is equipped with a little storage space, which it uses to coordinate its activities with those of all the other units. One of the most important parts of a sensor node is the power unit, which is responsible for connecting all of the other parts. The last component that connects the sensor nodes to the network is the transceiver unit. This component includes both a transmitter and a receiver.In idle mode, the transceiver consumes about the same amount of power as it does in transmit and receive mode. As a result, power consumption may be minimized by turning off the transceiver in

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3806-3821
https://publishoa.com
ISSN: 1309-3452

idle mode. It also features a location locating system, mobilizer, and power generator, depending on the application needs [1].

1.1 The WSN Security

Because of the following reasons, WSN security is a critical need for sensor networks (Walters et al. 2006) [3:]

i. Sensor networks handle sensitive data, such as military and healthcare applications.
ii. Many resource limits exist in sensor networks, such as low latency, storage space, and processing capabilities.
iii. Because the sensor network uses needed areas and connectionless packet-based transmission, data transfer is unstable.
iv. Sensor nodes are placed in an unattended environment and are monitored remotely by administrators. As a result, attackers may simply physically compromise them.

1.2. WSN Attacks

In general, assaults are divided into two types: active and passive. Active assaults disrupt the network's regular communication and alter data transmission. Sinkhole attacks, packet dropping, and IP spoofing are among the examples. Passive attacks gather data without interfering with network transmission and traffic management, traffic analysis, and eavesdropping. Lupu (2009) defines formalized attacks in Wireless Sensor Networks [4], Formal paraphrase Below is a taxonomy of assaults based on the Open System Interconnection model layers (Huang et al. 2010) [5].

(i) Physical layer attacks.

Node failure attack–A node failure may occur due to physical damage to the sensor node, hardware failure, or software failure.

Jamming attack–The jammer device sends radio signals and disrupts the sensor network's communication channel.

ii) MAC layer attacks

Traffic modification attack–The attacker provides bogus data or prevents all data from passing over a communication link.

iii) Sybil attack–An identity spoofing assault is also known as a Sybil assault. It is because the attackers impersonate a valid sensor by duplicating the node IDs.

iv) Network layer attacks

Packet replication–The attackers transmit the identical packet to the recipients that were previously delivered to them. It consumes much energy in the sensor network.

Sinkhole attack: The attackers notify the sensor nodes of the erroneous route. The sensor views a fake route as an ideal route and directs all traffic via it.

Packetdropping**:** The attackers may drop a packet selectively or entirely.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3806-3821
https://publishoa.com
ISSN: 1309-3452

Routing attack**:** The attacker broadcasts the erroneous routing route to the correct nodes.

Hello, flood attack: The attackers send a hello packet to each of the adjacent nodes. As a result, the genuine node forwards the packet to the attacker, thinking the attacker is a neighbor.

v) Application layer attacks

Changes to data aggregation–Data acquired at sensors is transmitted to aggregators for additional processing. Data aggregation is computed by the aggregators and sent to the BS. The attackers, however, manipulate the data aggregation and insert erroneous aggregate values.

2. Data Aggregation and Security Background

A strategy known as data clustering is one that has the potential to cut down on the transmission overhead in a Wide-area Network (WSN). Because of the nature of the data that is acquired by sensors, ensuring that the network is safe is of the utmost importance. Data aggregation is the method through which this goal is accomplished. The effectiveness of the hackers who are trying to break into the network is one of the primary contributors to the network's susceptibility to attack [6].

The most recent generation of algorithms does not meet the required level of safety, despite the fact that data aggregation has a variety of beneficial effects. Instead, they depend on a cryptosystem that is homomorphic to do the aggregation on their behalf. Because it does not need the employment of a cluster head to decode the data, this technique consumes less power than others.The purpose of this study is to offer a technique for authenticating and encrypting data at the BS that incorporates two different methods: the Paillier additive homomorphic approach and the Bilinear aggregate signature. Wide-area networks are often used in a variety of applications, including those involving open environments and sensitive data, such as health monitoring and surveillance systems. They are made up of nodes, which are often classified as either sensor nodes or sink nodes, depending on their function. Even though these sorts of nodes seem to be computers, they only have a small amount of memory and restricted processing capabilities.

Direct data transmission from sensor nodes to sink nodes uses up more energy than indirect data transfer since sensor nodes have less resources than sink nodes. When it comes to gathering data in a centralised fashion, the sink node serves as the starting point of the process [7].

As a direct consequence of this, WSN consumes a greater quantity of energy in order to process the data obtained from the sensors. A number of the aggregation

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3806-3821
https://publishoa.com
ISSN: 1309-3452

functions may be carried out by the cluster heads themselves in certain circumstances. On the other hand, the aggregation is often carried out by the standard nodes themselves [8].

The sum, max, and min function is one of the most frequent aggregation functions that is done, and it is useful in computing the average temperature since it helps determine the range of temperatures. During this stage of the process, the information gathered by the sensors and the different values obtained from the sink node are merged together.The network's overall energy usage might be lowered by as much as 70 percent if only the right data were aggregated. However, it is still very necessary to make sure that the data's security is maintained via the use of data aggregation in order to avoid any potential problems. The ability to prohibit unwanted access to the data that is acquired by the sensors is one of the most significant issues that wireless sensor networks (WSNs) confront. In military applications, cyberattacks against sensor nodes are still regarded to be threats to national security, despite the fact that they may have the ability to endanger a person's life [9].

The process of data aggregation may leave a company open to a wide range of threats, including those posed by black holes, eavesdropping, and collisions, to name just a few. It is essential, in order to avoid unwanted access to the data that has been acquired, that the security of the data be maintained via the use of procedures that are designed to aggregate secure data. Among them are the capabilities of adding new data, authenticating users, and maintaining data secrecy.Utilizing a mobile device, a person is able to gather and send data about their movements and characteristics to a data sink while using a system called the body area network (BAN). Figure 1 presents a visual representation of the system's four distinct stages. After then, both the master key and the shared key are sent to each and every node in the network [10].

The first thing that has to be done in order to complete the procedure is to generate private keys depending on the characteristics of the user. In step 3, the process encrypts the message by using CP-ABE in conjunction with AES. In step 4, the consumers of the data, such as nurses and physicians, are responsible for decrypting the information in order to get the session key.

In spite of the complexity of the system, it is nevertheless in a position to guarantee the safety of a number of different users and sensors. In addition, the cost of maintaining the system is rather high.

The physiological data of the user, such as their ECG and blood glucose levels, are being continually monitored by the body sensor nodes. After then, the data are sent through

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3806-3821
https://publishoa.com
ISSN: 1309-3452

Bluetooth to the mobile device that is associated with the user. The personal digital assistant makes use of steganography technology in order to conceal the data.After that, the information is sent to the hospital over the internet. By using this strategy, we guarantee that only authorised medical professionals may see the patient's medical records [11].

3. Homomorphic Encryption in Wireless Sensor Networks

Homomorphic systems, in contrast to other varieties of encryption, are better equipped to deal with a variety of data formats. When it comes to the transfer of medical data, there are a variety of requirements that need to be satisfied in order to guarantee the data's privacy and safety. Recovering each and every piece of data, ensuring that the data is secured on the device used by the physician, and maintaining a reasonable price are some of these considerations.

The use of blowfish encryption provides an alternative to the conventional approaches that are often used to secure the confidentiality of medical data. The Wearable Medical System Network (WMSN) is responsible for the collection of data from biosensors that are attached to a patient's body in order to monitor the patient's physiological condition. After that, the information is sent to a diagnostic centre [12].

After the data has been gathered by the sensors, it is sent to the device used by the doctor so that it may be analysed. Unauthorized access to the data might result in a variety of legal difficulties and possibly put patients' lives in jeopardy if the appropriate authorisation is not there [13].

The criteria for network security imposed on WSNs are comparable to those imposed on conventional networks. In order to ensure that the data is secure, in addition to factors such as confidentiality, integrity, availability, and network secrecy, other considerations, such as the authenticity and freshness of the data, are also taken into account. Authenticity and freshness of the data are examples of such considerations. Despite the many different kinds of study that are being carried out on the topic, there are researchers that have exclusively concentrated on the secrecy and integrity of the data [14].

The goal of the Safe and Individualized Healthcare System that has been presented is to deliver a healthcare experience that is both secure and personalised. This is accomplished by combining the different security criteria of the WSN with access control approaches.

3.1 Protocols Used for Controlling Access

Applications used in the healthcare industry are required to have a high degree of security in order to safeguard the sensitive data that they contain. This information is accessible to

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3806-3821
https://publishoa.com
ISSN: 1309-3452

a broad variety of users, including patients, medical professionals, and nursing staff members. Unauthorized access to the data might result in a variety of legal difficulties and possibly put patients' lives in jeopardy if the appropriate authorisation is not there.

An access control approach is a sort of security that enables individuals to restrict unwanted access to the data that they maintain. This type of protection was developed by the National Security Agency (NSA). It is possible to utilise it to provide different kinds of access permissions to users, based on the responsibilities of those users.

(i) Management of access privileges depending on roles.

It is possible for educational institutions and businesses to use role-based access control in order to provide certain groups with access to specific information. These organisations will then have access to the information that will allow them to make choices based on accurate information. When hundreds of things and themes are accessible, it might be advantageous for an organisation.

(ii) Access control while maintaining the confidentiality of user information

Users' privacy may be protected in a multi-user system by the implementation of an access control approach, which grants users permission to see certain information based on the requirements of their particular use cases. After that, the network administrator assigns the group a group id and a group signature to use moving forward. Nevertheless, this approach may prove to be rather useful in situations in which the number of group members exceeds the available identifiers for the groups.

(iii) A security system that relies on cryptography for access control

It is possible for a group of users to collaborate in order to generate a secret key that may be used to get access to the data. Applications in both the military and the medical field often make use of this particular kind of access restriction. Persons are able to stop unauthorised people from accessing the data that they save on their computers by using a kind of security known as attribute-based encryption.

The ABE system exhibits a diverse collection of traits over its whole. Approaches for controlling access include key-policy, threshold-policy, ciphertext-policy, and non-monotonic policy control. These are the four categories of access control techniques.

The user and the ciphertext may both be identified with the use of a method known as threshold policy access control. The user is able to decode a ciphertext if the user's private key satisfies the threshold characteristics that have been established for the ciphertext. A kind of security that is known as fuzzy identity-based encryption is one of the most prevalent forms of access control

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3806-3821
https://publishoa.com
ISSN: 1309-3452

mechanisms. This form of security is also known as security.

Due to the fact that it combines a private key with a set of characteristics, the employment of key-policy or threshold-policy leaves users open to the possibility of collusion attacks. However, since the system administrator has very little control over who may access the data, this sort of protection is often only used in circumstances in which the key is very important.

The fact that the properties of a ciphertext policy are tied to the keys that it includes makes it much simpler for the owner of the data to figure out who is authorised to access the information. This sort of security is also more adjustable since it is possible to alter the structure of how access is granted to the system.

3.2 Controlling access to policies via the use of non-monotonic policies:

Controlling a non-monotonic policy has many of the same qualities as controlling a monotonic strategy. However, rather than limiting access to the data itself, this sort of security gives specific users a negative expression in order to stop them from decrypting the ciphertext.

A homomorphic encryption method generates an encrypted result that is equivalent to the outcomes of an operation that was carried out on the plaintext. Each sensor node in the network is responsible for storing the encryption key prior to transmitting the unencrypted data to a higher-level node. Following that, the higher-level node decrypts the ciphertext that it has received and sends it on to the subsequent higher-level node.

After the procedure has been carried out up till the BS has been reached, the ciphertext is decoded in order to reveal the outcomes of the operation. In many different areas, including cloud computing and wireless sensor network data aggregation security, homomorphic approaches are employed often.

The sum of two ciphertexts and the exponential property are the two sorts of variations of homomorphism that occur most often in everyday use. The method of creating two ciphertexts, which subsequently returns the plaintexts of those ciphertexts, is referred to as the exponential property. In order to get the best results with classical homomorphic encryption at the lowest possible cost, it was decided to make use of the Paillier algorithm.

In comparison to the other forms of homomorphic encryption, the Paillier method presents a higher level of difficulty in terms of its performance. Because of this, the technique is only carried out on the server's side of the connection.

To illustrate the performance of a dependable data aggregation system in WSN by using the Paillier algorithm is the primary objective of this work. Through the use of the bilinear

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3806-3821
https://publishoa.com
ISSN: 1309-3452

approach, the data is sent to Bs. At each individual sensor node, the process of signature creation is carried out according to the bilinear technique.

The data is subsequently sent from the sensor node to the cluster head, which is responsible for receiving the encrypted digital signature and decrypting it. This guarantees that the data's validity and secrecy are preserved throughout the whole process, from beginning to conclusion.

Algorithm-1:Key Generationalgorithm

Step 1: Choose randomly large prime numbers, p, and q.

Step 2: Calculate $\gcd(pq,(p-1)(q-1))=1$

Step 3: Calculate $\lambda = lcm(p-1,q-1)$

Step 4: Select random integer g such that $g \varepsilon Z_n^{*2}$

Step 5: Check n divides g by using $\mu = \left(L\left(g\lambda \bmod n^2\right)\right)^{-1}$ as $L(u) = (u-1)/n$

For the encryption of public key pair is (n, g) and for the decryption of private key pair is (λ, μ).

Algorithm-2: Encryption algorithm:

Step 1: Let m plain text message be considered as m ε Zn

Step 2. Select random r where r ε Z_n^*

Step 3. Calculate ciphertext $c = g^m r^n \bmod n^2$

Algorithm-3: Decryption algorithm:

Step 1: Let C Ciphertext message be considered as C ε Z_n^{*2}

Step 2. Plain Text Calculation $m = \left(L\left(c^\lambda \bmod n^2\right).\mu \bmod n\right)$

Step 3 Calculate ciphertext $c = g^m r^n \bmod n^2$

$$D\left(E\left(m_1, r1\right)\cdot E\left(m_2, r2\right) \bmod n^2\right) = m_1 + m_2 \bmod n \text{ Eq-(1)}$$

$$D\left(E\left(m_1, r1\right)\cdot g^{m2} \bmod n^2\right) = m_1 + m_2 \bmod n \text{ Eq-(2)}$$

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3806-3821
https://publishoa.com
ISSN: 1309-3452

Equations 1 and 2 depict Homomorphic propertiesand the calculations of encryption functions of Two ciphertexts and ciphertext with a plaintext product, respectively.

4. Experimental Analysis and Discussion

The proposed Provably Secured Data Aggregation (PSDA) approach secures sensor data using two security techniques: The first is the Paillier homomorphism cryptosystem, while the second is the bilinear aggregate signature. The Paillier homomorphism cryptography protects against a chosen plaintext attack. The Bilinear aggregation signature technique is safe against the selected vital type attack, and no zero-knowledge proof is required. Because the PSDA approach incorporates both security approaches, it is likewise safe against the selected plaintext attack and selected critical model attack. Pallier homomorphic encryption also ensures data secrecy. Homomorphic encryption, in general, executes the clustering method on the ciphertext directly. In the cluster heads, the keys are not given to the outside world, resulting in end-to-end encryption and secrecy. Similarly, the Bilinear aggregate signature ensures legitimacy. The data integrity is also acceptable since if any of the ciphertexts is changed, the signatures at the BS in the verification step will not match.

The PSDA framework developed at the Intel lab was built with the help of the Net-Beans IDE version 7.3. Every 31 seconds, measurements of temperature, humidity, and light are taken using sensors that are known as Mica2 Dots. These sensors are being utilised for this research. The information gathered by the platform is subsequently included into the construction of a network.

The date, the epoch, the time, the temperature, and the mote id are the five factors that are used in this project. The measurements of the temperature have been encrypted. A PC equipped with a 2.66GHz Intel Core i5 CPU and 4GB of RAM is being used to carry out the research at this time. In spite of the fact that the central processing unit (CPU) is only marginally quicker than the sensor nodes, it is nevertheless able to illustrate the performance of the numerous methods that are engaged in the project.

The purpose of the effort is to devise a system that is both safe and effective for assessing the information that has been gathered by the sensors. Other methodologies, such as SIES, SEEDA, and EPSA, are evaluated alongside this framework and contrasted.

Table 1 and Figure 2 indicate the amount of time required to decode the data. Table 3 and Table 4 show the amount of time required to decrypt and aggregate the data, respectively.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3806-3821
https://publishoa.com
ISSN: 1309-3452

In addition, the number of cluster heads is presumed to be one and ten, respectively. The duration of time that is used by the system is quantified in seconds.

The time it takes to generate, encrypt, and compile the data is included into the total amount of time needed for the computation. The length of time necessary to collect the data and signatures from each of the cluster heads is referred to as the "aggregation time."

Table-1: Encryption Time of Proposed PSDA with Others

	Encryption			
File size (in KB's)	SIES (s)	EPSA(s)	SEEDA (s)	PSDA (s)
10	1.8	1.68	0.96	1.32
20	2.4	1.8	1.08	1.56
30	3	1.92	1.2	1.8
100	3.6	2.4	1.44	2.16
150	3.6	3.12	1.56	2.4
400	9.6	7.44	2.76	5.04
600	11.4	10.2	4.8	7.8

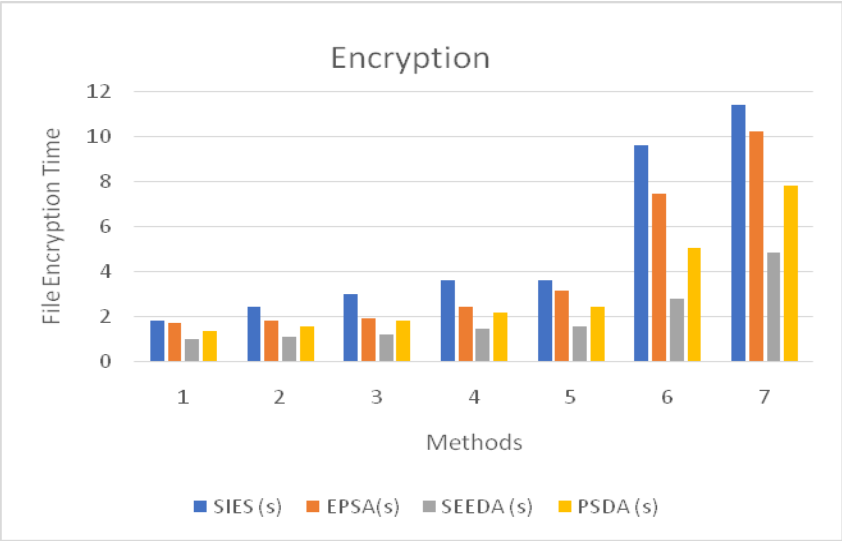

Figure 2: Comparison of Encryption Time of Proposed PSDA with Others.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3806-3821
https://publishoa.com
ISSN: 1309-3452

Table-2: Decryption Time of Proposed PSDA with Others

	Decryption			
File size (in KB's)	SIES (s)	EPSA(s)	SEEDA (s)	PSDA (s)
10	2.16	2.04	0.84	1.92
20	15.12	12	6	10.8
30	15.6	13.2	7.44	12
100	18.72	15.6	9.6	14.4
150	21.84	18	12	16.8
400	43.2	39.6	26.4	37.2
600	45.6	43.2	30	39.6

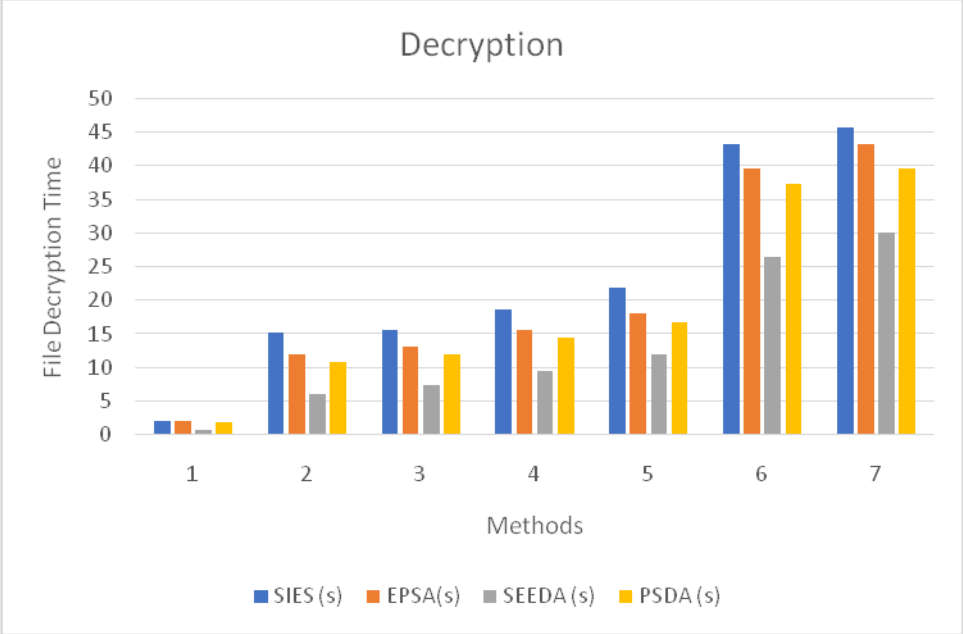

Figure 3: Comparison of Decryption Time of Proposed PSDA with Others

Table-3: Total computation time of Proposed PSDA with Others

	Total computation time			
File size (in KB's)	SIES (s)	EPSA(s)	SEEDA (s)	PSDA (s)
10	4.8	4.2	2.28	3.6

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3806-3821
https://publishoa.com
ISSN: 1309-3452

20	19.2	15	7.2	13.2
30	19.8	16.8	9.6	14.4
100	24	19.2	12	18
150	30	24	15.6	21.6
400	58.8	51.6	31.8	45.6
600	64.8	60	39.6	52.8

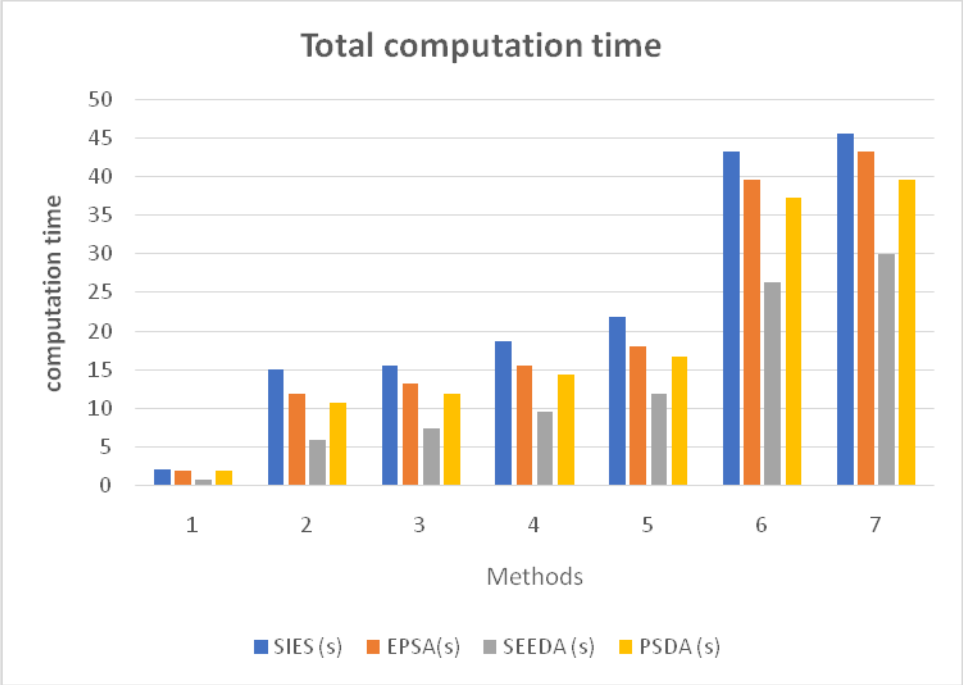

Figure 4: Comparison of Total computation time of Proposed PSDA with Others

According to the comparison, the SIES methodology takes extra encryption and decryption time owing to the sensors and cluster head producing a unique RSA signature. Additionally, since signature verification is conducted individually at the BS, more calculating time is required. Because the EPSA technique includes an additional header field at each level, it needs more time for encryption and decryption than PSDA. SEEDA, on the other hand, requires less time to encrypt, decrypt, and aggregate than any of the other approaches since it does not include a verification method. One of the benefits of adopting a homomorphic encryption technique is that it needs less time to be secured and decrypted than other algorithms.

A wireless sensor network is a form of network that is useful for a variety of purposes, including industrial monitoring, transportation monitoring, and disaster management monitoring. It is possible

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3806-3821
https://publishoa.com
ISSN: 1309-3452

for it to be made up of sensor nodes that use less electricity. These nodes are able to interact with one another and provide the central database with the data that they collect.

Because sensors have limited resources, they are an ideal target for attackers to take advantage of. By physically tampering with the nodes that make up these devices, for instance, attackers may get access to the data that is stored on those devices. They also have the ability to change or discard data packets.

The data collected by sensors may be protected by a wide variety of security methods; nevertheless, these safeguards are not capable of preventing every possible kind of intrusion. Because of this, it is essential for there to be an IDS installed in the WSN so that it can screen out irregular packets.

The majority of the examinations that are being carried out on IDS and sensors right now are concentrating their attention on the network layer. On the other hand, they don't take into account the other layers. In this concept, it is suggested that a rule-based intrusion detection system (IDS) be used to filter the assaults that are made against the sensor nodes. It is possible for this strategy to block the transmission of the packet to the central database. The learning machine known as the Extreme Learning Machine served as the inspiration for the algorithm that was suggested.

The findings of the simulation indicate that the various classification methods, including the ELM, BPN, and SVM, performed admirably when applied to the NSL-KDD database. In addition, in comparison to the other approaches, the ELM algorithm was able to recognise a greater number of abnormalities. Following this step, two sensor nodes are placed in the testing environment in order to capture data in real time.

5. Conclusions

WSN is being employed in a wide range of applications. WSN data security and energy usage are major research topics. The present study's primary goal is to create a revolutionary algorithm for ensuring data security while using less energy. This proposal discusses the research results, the importance of the research contribution, a summary of the research activity, and the potential for future investigation. The computing time of security methods is closely related to network energy usage. As a result, the suggested security approaches focus on delivering security attributes such as data integrity, secrecy, and authenticity while requiring minimal computation time. A thorough investigation is conducted to identify the best end-to-end encryption method and aggregate signature approaches for safeguarding sensor data. The Intel lab dataset is used to create the combination of algorithms for temperature measurements. A homomorphic cryptosystem's drawback is that it is not recoverable and is not suited for a block of diverse data kinds.

Volume 13, No. 3, 2022, p. 3806-3821
https://publishoa.com
ISSN: 1309-3452

Homomorphic cryptosystems also have a long decryption time. Because the decryption is performed at the BS, the decryption cost is omitted in the application. One of the primary uses of WSN is the remote patient monitoring system. Misuse or delay of health data might complicate matters for patients. The monitored health data must reach medical repositories and clinicians swiftly and securely.

Decrypting medical data of various data kinds takes a long time using homomorphic cryptosystems. As a result, research is conducted to identify the best symmetric algorithm and access control approaches. Blowfish and CP-ABE are chosen as the best and tested on gender, body temperature, and cardiac rate parameters. Lightweight symmetric algorithms are intensively studied in order to minimize computing time for low-powered devices. Speck and CP-ABE are later linked to being an appropriate mix and carried out on health data. The bulk of current intrusion detection systems (IDS) are designed to detect network layer assaults rather than cross-layer assaults. Following then, the study has concentrated on providing IDS for cross-layer threats. To execute this assignment, research of assaults, the effects of assaults, and criteria to identify assaults is conducted.

References:

[1]. Mackowiak, PA, Wasserman, SS & Levine, MM 1992, "A Critical Appraisal of 98.6 Degrees F, the Upper Limit of the Normal Body Temperature, and Other Legacies of Carl Reinhold August Wunderlichs', Journal of the American Medical Association, vol. 268, no. 12, pp. 1578-1580.

[2]. Akyildiz, IF, Su, W, Sankarasubramaniam, Y &Cayirci, E 2002, Asurvey on sensor networks, IEEE communication magazine, vol. 40,no. 8, pp. 102-114.

[3]. Walters, JP, Liang, Z, Shi, W & Chaudhary, V 2006, Security in distributed, grid, and pervasive computing, CRC Press: Boca Raton, FL, USA.

[4]. Lupu, TG 2009, "Main types of attacks in Wireless Sensor Networks', Proceedings of the 9th WSEAS International conference on signal, speech and image processing, pp. 180-185.

[5]. Huang, YM, Hsieh, MY, Chao, HC, Hung, SH & Park, JH 2009, "Pervasive, Secure Access to a Hierarchical Sensor-Based Healthcare Monitoring Architecture in Wireless Heterogeneous Networks', IEEE Journal on Selected Areas in Communications, vol. 27, no. 4, pp. 400-411

[6]. Claude, C, Aldar, CFC, Einar, M & Gene T 2009, "Efficient and provable secure aggregation of encrypted data in Wireless Sensor Networks', ACM Transaction on Sensor Networks, vol. 5, no. 3, pp. 1 – 36.

Volume 13, No. 3, 2022, p. 3806-3821
https://publishoa.com
ISSN: 1309-3452

[7]. Stavros, P, Aggelos, K & Dimitris, P 2012, "Exact In-Network Aggregation with Integrity and Confidentiality', IEEE Transactions on Knowledge and Data Engineering, vol. 24, no. 10, pp. 1760-1773.

[8]. Hu, C, Li, H, Cheng, H & Liao, X 2015, "Secure and Efficient data Communication protocol for Wireless Body Area Networks', IEEE Transactions on multi- scale computing systems, vol. 11, no. 14, pp. 1-11.

[9]. Ibaida, A & Khalil, I 2013, "Wavelet-Based ECG Steganography for Protecting Patient Confidential Information in Point-of-Care Systems', IEEE Transactions on Biomedical Engineering, vol. 60, no. 12, pp. 3322 – 3330.

[10]. Alemdar, H & Ersoy, C 2010, "Wireless sensor networks for healthcare: A Survey', Computer Networks, vol. 54, no. 15, pp. 2688-2710.

[11]. Qiao, Z, Liang, S, Davis, S & Jiang, H 2014, "Survey of Attribute Based Encryption', IEEE International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/ Distributed Computing, pp. 1-6.

[12]. Sen, J 2013, Theory and Practice of Cryptography and Network Security Protocols and Technologies, Intech Publishers, Croatia, Europe.

[13]. Boneh, D, Gentry, C, Lynn, B &Shacham, H 2003b, "A Survey of Two Signature Aggregation Techniques', RSA cryptobytes, vol. 6, no. 2, pp. 1-10.

[14]. Stavros, P, Aggelos, K & Dimitris, P 2012, "Exact In-Network Aggregation with Integrity and Confidentiality', IEEE Transactions on Knowledge and Data Engineering, vol. 24, no. 10, pp. 1760-1773.