An Upgraded Data Security Based on Homomorphic Encryption and Aggregate Signature Method in Wireless Sensor Network

Raju Ranjan[1,*], Vinay Kumar Ahlawat[2]

[1]School of Computing Science and Engineering, Galgotias University, Greater Noida, India

[2]Department of ITSS, KIET Group of Institutions, Ghaziabad, India,

Emails: drraju.ranjan@galgotiasuniversity.edu.in; vinahlawat@gmail.com

Abstract

Wireless sensor networks (WSN) have been implemented in nearly every field of use because they offer a solution to practical problems that can also be affordably implemented. The sensor nodes have limited computing resources, weak batteries, and limited storage space. The environmental or physical data collected by these nodes is transmitted straight to the BS. The data transfer cost is raised due to the direct data transmission. In addition, the lifetime of sensor networks is shortened because of the rise in energy required for data exchange. As a result, data aggregation is utilized in WSN to lessen the burden of transmission costs and lengthen the useful life of the sensor networks. Each sensor node's transmission is encrypted with cipher text generated by the Paillier homomorphic cryptosystem. In addition, the Bilinear aggregate signature method is used to create a digital signature at each sensor node. The cluster head / BS is where the aggregation takes place once the cipher text and signature have been combined. Before deciding whether to accept or reject the message, the BS checks the aggregate signature. The homomorphic cryptosystem saves power because it does not perform intermediate-level or cluster-head decryption. Data integrity, authenticity, and confidentiality are all maintained while using less power with this technology. The Intel laboratory dataset is used in the implementation. When compared to current systems, the proposed SDA method requires less time and energy to calculate.

Keywords: WSN; Cipher text; SDA; Encryption;

1. Introduction:

The military, business, healthcare, and education are just some of the sectors that have used WSN in recent years. Hundreds or even thousands of sensor nodes are spread out across a given area and linked to a central Base Station (BS) in order to keep tabs on the environment. The sensor node collects data about its surroundings and sends it to the base station [1]. The BS then sends the data out to the users over the internet. The sensor network's adaptability, portability, durability, and reactivity make it a prime candidate for usage in a wide variety of applications [2].

The sensors collect data about the surrounding environment and send it to the ADC module, which keeps track of things like temperature, light, humidity, pressure, and so on. The analog-to-digital converter (ADC) takes the analog signals from the sensors and turns them into digital ones. The processing unit has limited storage space for coordinating with other units to carry out the operation. The power unit is the most critical part of a sensor node because it provides juice to everything else [3-4].

Doi : https://doi.org/10.54216/JCIM.120102
Received: December 04, 2022 Revised: January 20, 2023 Accepted: April 20, 2023

The sensor nodes communicate with the network via a transceiver device that serves as both a transmitter and a receiver. The transceiver's power consumption in standby is quite close to that of the transmit and receive modes. Power can be saved by turning off the transmitter while it's not in use [5]. It also features a locator, a mobilizer, and a power generator, all of which can be activated depending on the situation. Data transfer between sensor nodes in the field is impossible without a location-finding mechanism. The sensor nodes can be relocated to other areas with the help of the mobilizer unit [6].

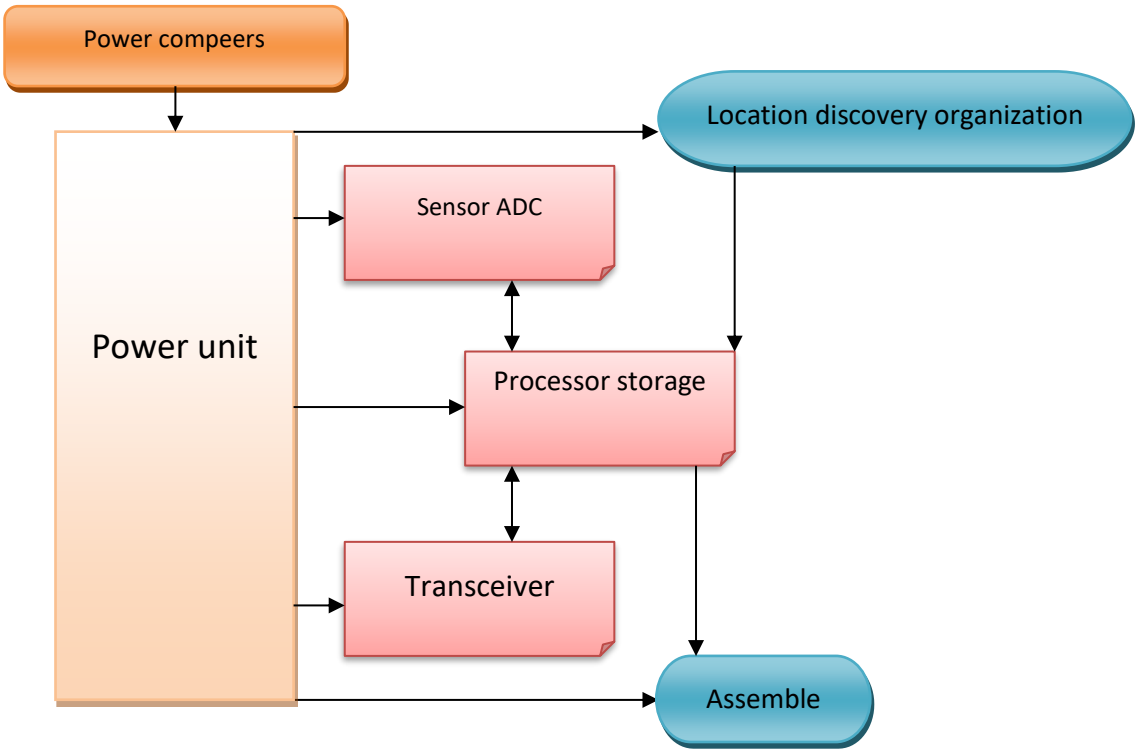

Figure 1: A sensor node Components.

For the reasons listed below, sensor network security is an absolute necessity.

i). When it comes to military and healthcare applications, sensor networks must deal with highly confidential information.

ii). Limited memory, storage space, and processing capabilities are just some of the resource restrictions faced by sensor networks.

iii). Administrators deploy sensor nodes in an unattended setting and take care of them from afar. As a result, their bodily safety is easily within the reach of their assailants [7].

For these reasons, conventional wireless network security measures are inadequate for protecting WSNs. Therefore, the security methods need to be improved while also requiring less resources (memory, processing, and transmission) to function. Because they rely on batteries to function, sensor nodes deployed in outlying areas can quickly die and are difficult to replace. Power is used more intensively at the sensor node because of its several functions. Sensors have a higher energy requirement for data transfer than computers. It takes the same amount of power to send 1 Kb of data 100 meters in a sensor as it would to execute 3 million instructions on a processor capable of 100 million instructions per second at 1 watt [8]. Using more juice while running complicated security algorithms is a given. The decrease in sensor node lifetime is a direct result of the rise in power consumption. Solar-powered sensor nodes are preferred over battery-powered nodes because of their ability to capture energy from the sun, but their performance is optimal only in daylight. Therefore, the security method must be developed in a way that results in a short running time. A longer lifespan for a sensor node would result from a decrease in execution time because it would use less computing power [9].

Doi : https://doi.org/10.54216/JCIM.120102
Received: December 04, 2022 Revised: January 20, 2023 Accepted: April 20, 2023

2. Related Work

All these techniques are geared toward securing sensitive information and protecting against threats. We present a strategy for disjoint multipath routing between nodes that minimizes energy consumption [10]. Once multiple paths from source to sink node have been identified, the sink node will initiate the route construction phase. When routing data to the sink node, the optimal path is selected from among the available multiple paths, and all nodes update their routing tables based on the public keys of their neighbours [11]. This method lengthens the lifespan of networks by preventing attacks like selective forwarding, byzantine attacks, and the selection of alternate routing in the event of a network failure. The technique also ignores threats at the physical and media access control (MAC) layers. Physical data routing and multimedia data routing are also not considered [12].

Each node in the proposed lightweight verification algorithm has several parents. Each child node relays its MAC address and message to its parent [13]. When transmitting to the BS, the parent node includes its own MAC set in the merged message. If the received message's MAC set matches the fused value, the BS will accept the message; otherwise, it will be refused [14]. This method's key benefit is that it eliminates the requirement for the BS to receive a separate authentication message from each node in the network [15-17].

Using tree topology, nodes are divided into groups of similar size using the divide-and-conquer strategy. Each group's hop-by-hop aggregation is calculated using the Commit-and-Attest principle, and the group aggregate is then sent to the BS [18-20]. The SDAP approach excels because it can be used with any aggregation function (avg, min, max, total, count, etc.) and yields absolutely no false positives. The approach uses a hop-by-hop encryption scheme, which exposes the keys at intermediate nodes. Therefore, there is a chance of a security breach occurring [21-24].

The biometric method was developed by the authors as a way to both protect the network's keys and uniquely identify individual sensor nodes. From electrocardiogram and photoplethysmogram readings, the I.P.I. of a heartbeat can be determined [25-27]. The binary entity identifier for the sensor nodes in the BSN is derived from the Inter Pulse Interval. In telemedicine and m-health applications, the biometric trait is utilized to ensure the data's integrity, validity, and privacy.

It has been pointed out by the research community that while a central agent use decision tree approaches at the BS level, a local agent employs threshold-based metrics at the mote. The local agent will alert the main agent if it notices something out of the ordinary [28]. If the warning information provided by the local agent is verified, the central agent will relay its decision to all of the local agents. Sinkhole and sleep deprivation attacks can be uncovered with the help of the centralized agent [29].

3. The Proposed Model

In this investigation, we make use of the Paillier additive homomorphic cryptosystem in conjunction with the Bilinear aggregate signature method in order to encrypt and verify aggregate data at the BS. A sort of asymmetric encryption known as homomorphic encryption is one in which computations are carried out on cipher text in order to produce an encrypted result. This encrypted result, once it has been decoded, corresponds to the same results as operations carried out on plaintext. Before being sent to the next higher-level node or base station, the raw data in a sensor network is encrypted at each node. This occurs before the data is transmitted. The higher-level node performs processing on the cipher text as it arrives, and then sends it on to the subsequent higher-level node for processing. The BS is where the results of this kind of calculation are ultimately stored. At long last, the BS deciphers the cipher text, which reveals the results of the operations performed on the plaintext. The Paillier cryptosystem is an additive homomorphic cryptosystem. In this type of system, the value of (m1+m2) can only be determined if the receiver is also provided the public key as well as the encrypted values of m1 and m2. A simplified alternative of the overhead key creation procedures would be to set p, q to be the same length.

$$h = n + 1 \quad (1)$$

Doi : https://doi.org/10.54216/JCIM.120102
Received: December 04, 2022 Revised: January 20, 2023 Accepted: April 20, 2023

$$\delta = \emptyset(n) \quad (2)$$

$$\gamma = \emptyset(n)^{-1} \quad (3)$$

$$\emptyset(n) = (p-1)(q-1) \quad (4)$$

3.1. Encryption:
i). Let there be an encrypted message, m.
ii). Choose at Shuffle

iii). The Cipher text is calculated.

3.2 Decryption
i). Deciphering the cipher text, c
ii). Determine the unencrypted message.

Applications where aggregation functions such as sum, average, count, min, max, median, and variance are needed can benefit from the proposed Secured Data Aggregation (SDA) approach. The detection of forest fires is used as an example. The WSN's crucial function in forest fire detection cannot be overstated. Sensors for monitoring temperature, humidity, smoke, and gas levels have been placed throughout the forest. All of these sensors gather information and transmit it wirelessly to the BS or cluster head. The loss of even a single piece of this information could have catastrophic effects on the ecosphere. In addition, WSN resources would be further depleted if data transmission to the BS was required. End-to-end encryption is utilized in SDA to accomplish both of these goals while also reducing the system's overall power consumption.

The metrics required to track the forest fire are average, minimum, and maximum temperatures as well as humidity, gas, and smoke levels. Since Paillier homomorphic encryption is an additive homomorphic encryption method, it is the one selected by SDA. Paillier homomorphic encryption allows for the addition of temperature, humidity, smoke, and gas variables. The computation of average, minimum, and maximum may all be derived from the total. Bilinear aggregate signature method is used for authentication in the SDA.

Encryption and Decryption Method:

1. Use the Paillier cipher to turn a message into cipher text

$$c = g^m r^n mod n^2 \quad (5)$$

2. Find the secret message in the cipher text, m as

$$\varphi = (L(c^{\varphi} mod n^2).\mu \; mod \; n) = m \quad (6)$$

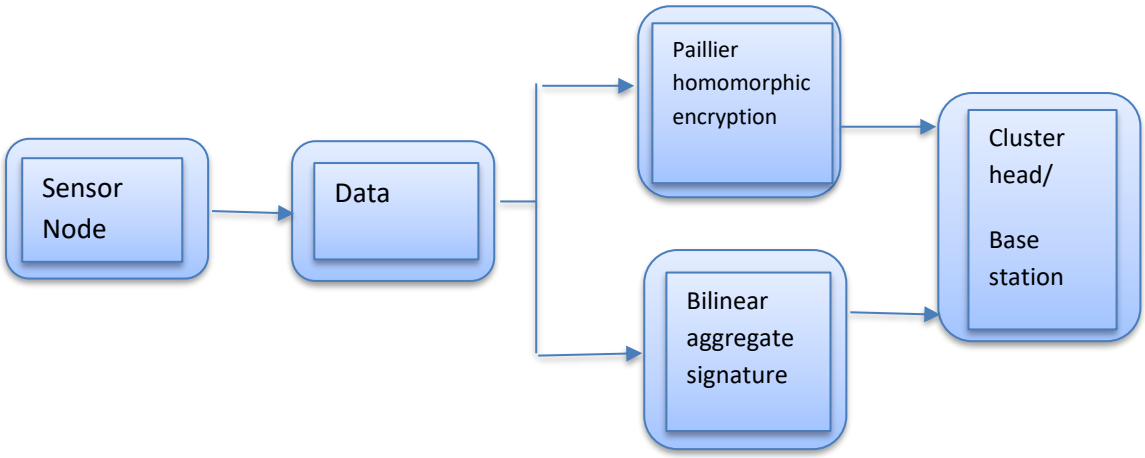

Figure 2: Statistics treating at individual sensor node.

Doi : https://doi.org/10.54216/JCIM.120102
Received: December 04, 2022 Revised: January 20, 2023 Accepted: April 20, 2023

3. The cluster master compiles cipher text from cipher text generated by all source nodes.

Decryption at BS: The Paillier homomorphic property states that adding the plaintexts of two cipher texts together yields the original messages. In this case, the summation of altogether messages (m_1, m_2,.....m_n) for sensor nodes 1, 2,..... n is intended by proliferating c1. c2..... cn. The Bilinear aggregate signature approach is used for verification.

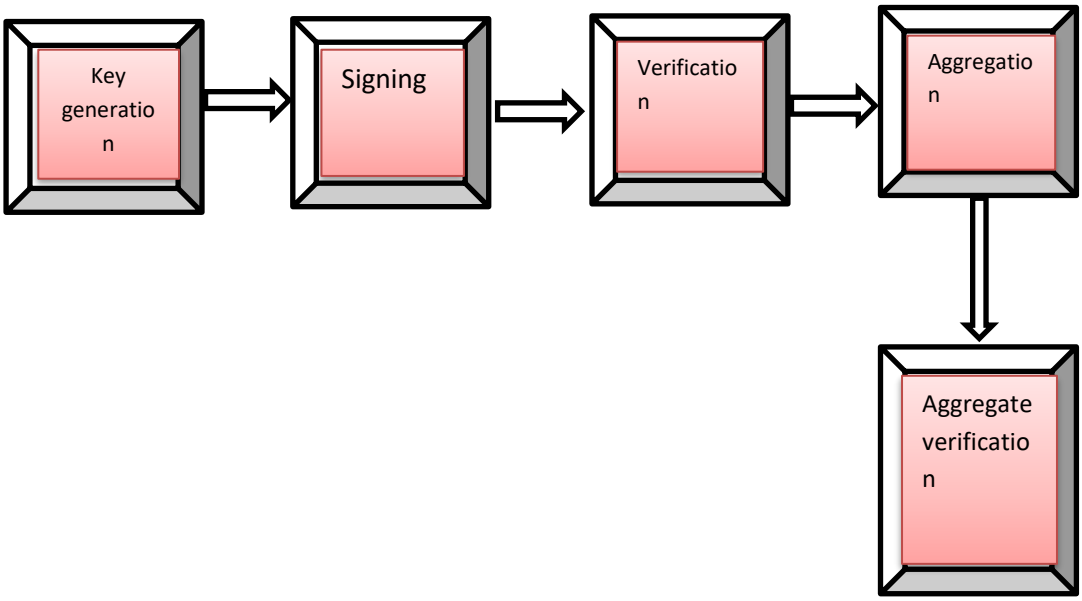

Figure 3: Bilinear aggregate signature method.

Digital signatures that allow for aggregation include the bilinear aggregate signature. It validates the signature encrypted into cipher text C for a specific message M. It creates signatures for any number of randomly selected messages. It uses a bilinear mapping structure.

In addition to their use in election methods, safeguarding data aggregation in WSN, protecting mobile agents, and cloud computing, homomorphic techniques have found application in other areas as well. Here are examples of two different kinds of homomorphisms:

i). When two cipher texts are added together and decrypted, the result is the same plaintext as the total of the cipher texts.

ii). When two cipher texts are multiplied together after decryption, the result is the product of their plaintexts; this property is known as multiplicative homomorphism.

Since the Paillier homomorphic cryptosystem has a lower encryption cost than other standard homomorphic encryption methods, it was selected for use in this investigation. Due to the Paillier's more involved and server-side-only decryption technique, it is typically disregarded.

Data privacy is ensured through Paillier homomorphic encryption. In most cases, the cipher text itself is what undergoes the aggregation process in homomorphic encryption. This end-to-end encryption ensures privacy by never letting the keys out of the system, not even to the cluster nodes. The Bilinear aggregate signature is another form of authentication. Since the verification at the BS would fail if the cipher text did not match the signature, the information veracity is also acceptable.

Doi : https://doi.org/10.54216/JCIM.120102
Received: December 04, 2022 Revised: January 20, 2023 Accepted: April 20, 2023

4. Experimental Results

Based on the current body of knowledge, the execution is carried out on a processer system featuring a 2.66 GHz Intel core i5 CPU and 4 GB of RAM. Though central processing unit performance is superior to that of actual sensor nodes, the latter can be used to illustrate the former's allied methods' efficacy. Existing systems such as Secure In-network processing of Exact Sum queries (SIES) and Secure End-To-End Data Aggregation (SEEDA) are used as comparisons to the SDA.

The encrypted result from homomorphic encryption, if decoded, corresponds to the sensor results of operations carried out on the plaintext. The raw data collected by each sensor node in a network are transmitted to the BS in an encrypted format. Following the completion of the cipher text processing, the higher-level node transfers it to the subsequent highest-level node. This computation goes all the way to the bottom of the stack. The output is converted into cipher text by the BS once it has been processed using the plaintext.

The encryption time is displayed in table 1 and figure 2, the decryption time is displayed in table 3 and figure 4, the aggregation time is displayed in table 4 and figure 5, and the total computing time is displayed in table 4 and figure 5. Various file sizes (15, 30, 120, 155, 420) are analysed and compared with regards to their internal temperatures. Here, we suppose that there are 10 nodes. Seconds (s) are used to measure the time spent waiting. The sum of the times it takes to generate a key, encrypt data, generate a signature, collect data, decrypt data, and verify data is the total computing time. The aggregation time is the sum of all the times that the cluster leader adds up all the data and signatures.

Table 1: Calculation of Encryption time based on variable size of file.

Algorithms	**File Size**				
	15	30	120	155	420
SIES (S)	2	2.4	3.2	3.4	8.2
SEEDA (S)	0.8	1	1.3	1.5	2.4
SDA (S)	1.2	1.4	1.6	2.2	3.4

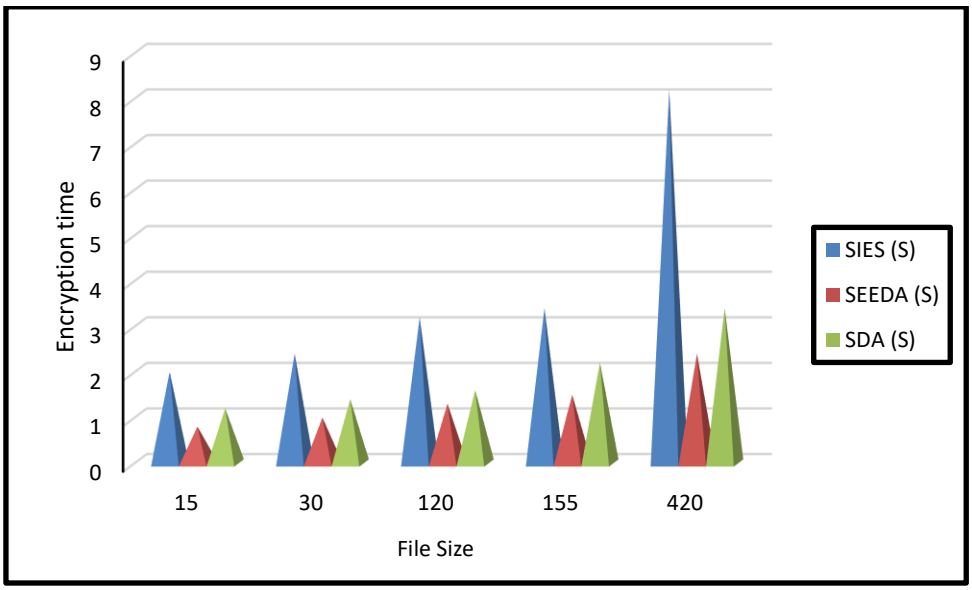

Figure 4: Calculation of Encryption time based on variable size of file.

Doi : https://doi.org/10.54216/JCIM.120102
Received: December 04, 2022 Revised: January 20, 2023 Accepted: April 20, 2023

The important outcomes can be conclude from Table 1 and Figure 4. According to the findings of the comparison, using the SIES method to encrypt and decode data takes significantly longer than using any of the other two choices. This is because each sensor and the cluster head are required to establish their own individual RSA signature. In addition, more processing time is required due to the fact that every BS must independently validate signatures. SEEDA has faster timings for encrypting data than any of the other methods, which is due to the absence of a verification mechanism in its design. In a similar vein, as the SDA uses homomorphic encryption and aggregate signature methods, it takes significantly less time to perform these processes compared to the SIES.

Table 2: Calculation of Decryption time based on variable size of file.

Algorithms	**File Size**				
	15	30	120	155	420
SIES (S)	12.5	13.2	15.8	18.2	36.4
SEEDA (S)	4.8	6.2	8.6	10.7	22.3
SDA (S)	8.9	10.4	12.5	14.3	31.2

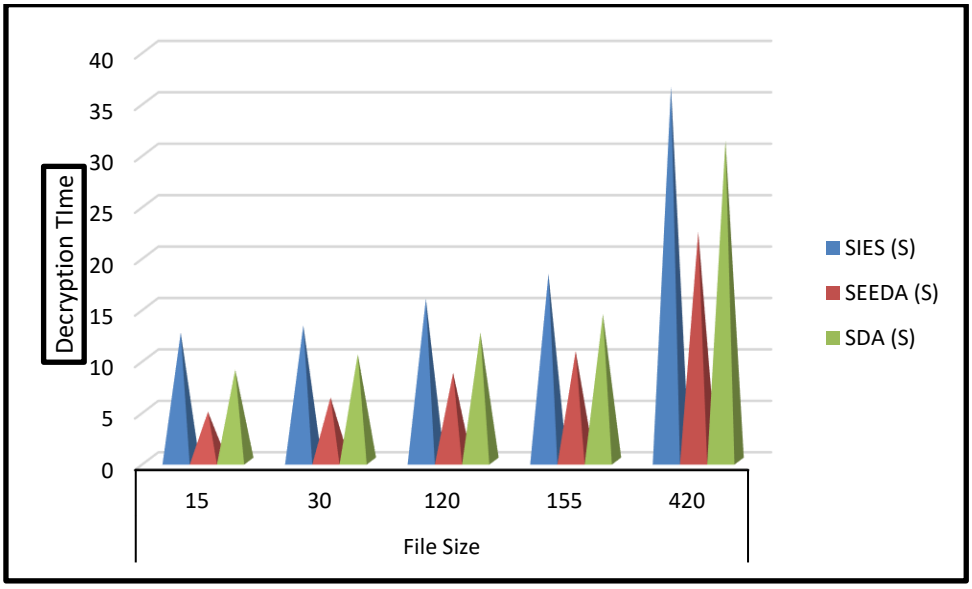

Figure 5: Calculation of Decryption time based on variable size of file.

Form Table 2 and Figure 5, it can be concluded that, SEEDA has faster timings for decrypting data than any of the other methods, which is due to the absence of a verification mechanism in its design. In a similar vein, as the SDA uses homomorphic encryption and aggregate signature methods, it takes significantly less time to perform these processes compared to the SIES.

Table 3: Calculation of Aggregation time based on variable size of file.

Algorithms	**File Size**				
	15	30	120	155	420
SIES (S)	0.26	0.39	0.74	1.63	3.15

Doi : https://doi.org/10.54216/JCIM.120102
Received: December 04, 2022 Revised: January 20, 2023 Accepted: April 20, 2023

SEEDA (S)	0.1	0.12	0.34	0.83	1.24
SDA (S)	0.21	0.16	0.24	1.15	2.17

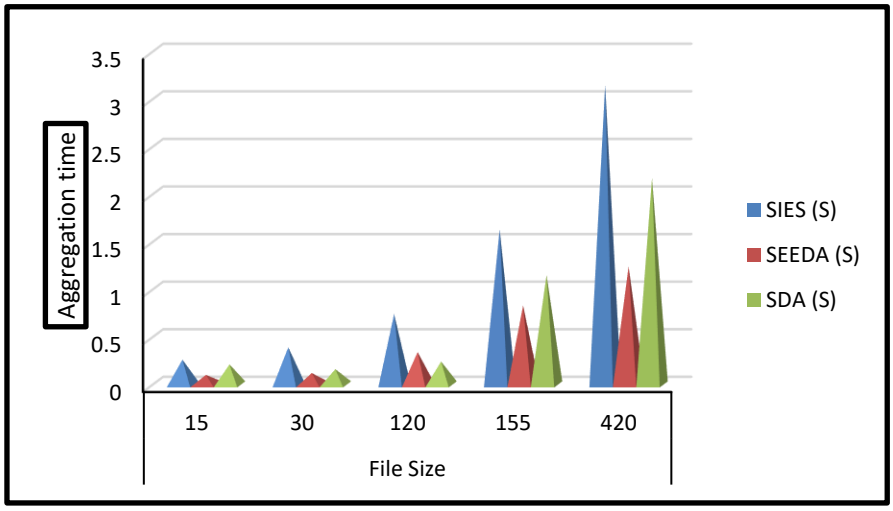

Figure 6: Calculation of Aggregation time based on variable size of file.

Table 3 and Figure 6 analysis gives suggestions that Due to the lack of a verification mechanism in its architecture, SEEDA has faster timings for encrypting, decrypting, and aggregating data than the other approaches. Similarly, the SDA's homomorphic encryption and aggregate signature methods allow it to do these tasks in a fraction of the time required by the SIES.

Table 4: Computation of Entire calculation time based on variable size of file.

Algorithm	**File Size**				
	15	30	120	155	420
SIES (S)	15.6	16.3	20.4	25.8	49.3
SEEDA (S)	6.2	8.5	10.6	13.8	26.7
SDA (S)	11.4	12.6	15.7	18.3	39.2

Doi : https://doi.org/10.54216/JCIM.120102
Received: December 04, 2022 Revised: January 20, 2023 Accepted: April 20, 2023

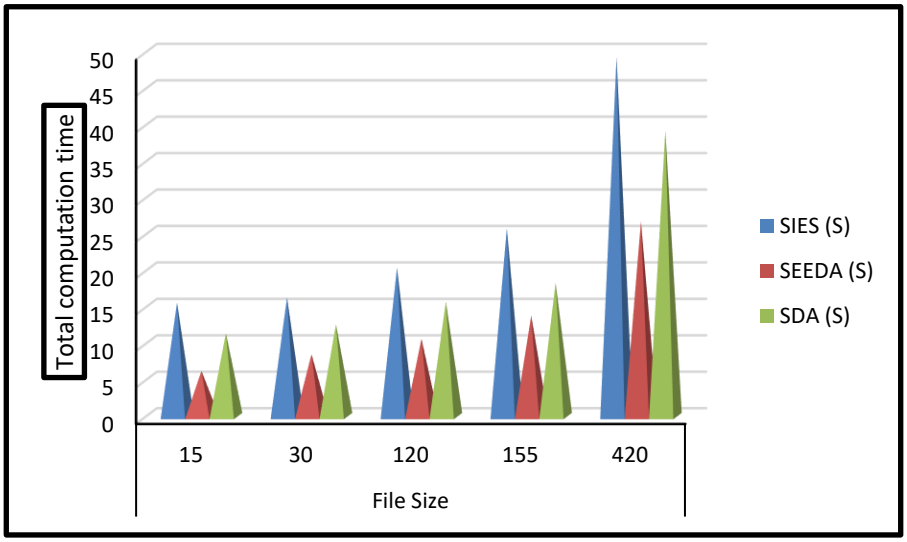

Figure 7: Computation of Entire calculation time based on variable size of file.

The comparison shows that the SIES technique requires more time to encrypt and decode data than the other two options since each sensor and the cluster head must generate their own unique RSA signature. In addition, more processing time is needed because each BS must verify signatures on its own. Due to its lack of a verification mechanism, SEEDA has faster encryption, decryption, and aggregation times than any of the other methods. Because it employs homomorphic encryption and aggregate signature methods, the SDA also requires less time for these operations than SIES. Due to its lack of aggregate signature, SIES requires extra processing time in both scenarios. Computational time is proportional to sensor node power consumption. If it's lower than that, it'll have a positive effect on the sensor nodes' ability to conserve power.

All the approaches aggregate and encrypt data with less energy expenditure than decoding. Energy usage can be disregarded because decryption will be handled at the BS. The sum of the energies expended during the processes of key generation, encryption, decryption, and aggregation constitutes the total energy footprint. When compared to SIES, SDA requires less power to perform encryption, decryption, and aggregation.

5. Conclusion

The current research makes use of WSN to compile encrypted data in a secure manner. The data's privacy can be protected with Paillier additive homomorphic encryption, while the data's integrity and authenticity can be safeguarded with bilinear aggregate signature. WSN is still able to make use of it despite the fact that it has a higher price tag due to the aggregate signature. A comparison of the performance of the SDA technique provided here with other methods that are comparable in terms of processing time and energy consumption demonstrates that the SDA method may be used in practice to aggregate data in a secure manner. WSN has seen an explosion in adoption rates within the healthcare sector over the past few years. In order to monitor the patient effectively, a large array of sensors are utilized. The homomorphic cryptosystem can only be used to encrypt data that is of a comparable type to the plaintext that is being decoded. This is necessary for the homomorphic cryptosystem to function correctly. Because there are many different types of data that need to be carried by the patient's data, the use of a homomorphic cryptosystem across all sensor data types would result in an increase in the costs associated with decryption. Because of this, the homomorphic cryptosystem ought not to be utilized in healthcare situations.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1]. Aggarwal, K, Saini, JK & Verma, HK 2013, "Performance Evaluation of RC6, Blowfish, DES, IDEA, CAST-128 Block Ciphers", International Journal of Computer Applications, vol. 68, no. 25, pp. 10-16.
[2]. Agrawal, DP (eds.) 2017, Embedded Sensor Systems, Springer Nature Singapore.

Doi : https://doi.org/10.54216/JCIM.120102
Received: December 04, 2022 Revised: January 20, 2023 Accepted: April 20, 2023

[3]. Akyildiz, IF, Su, W, Sankarasubramaniam, Y & Cayirci, E 2002, "A survey on sensor networks", IEEE communication magazine, vol. 40, no. 8, pp. 102-114.
[4]. Alassaf, N, Alkazemi, B & Gutub, A 2017, "Applicable Light-Weight Cryptography to Secure Medical Data In Iot Systems", Journal of Research in Engineering and Applied Sciences, vol. 2, no. 02, pp. 50-58.
[5]. Chen, CM, Lin, YH, Lin, YC & Sun, HM 2012, "RCDA: Recoverable Concealed Data Aggregation for Data Integrity in Wireless Sensor Networks", IEEE transaction on Parallel and Distributed Systems, vol. 23, no. 4, pp. 727 – 734.
[6]. Chew, LCN, Shah, INM, Abdullah, NAN, Zawawi, NHA, Rani, HA & Zakaria, AA 2015, "Randomness Analysis on Speck Family Of Lightweight Block Cipher", International Journal of Cryptology Research, vol. 5, no. 1, pp. 44-60.
[7]. Coppolino, L, Antonio, SD, Garofalo, A & Romano, L 2013, "Applying data mining techniques to Intrusion Detection in Wireless Sensor Networks", Proceedings of Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, pp. 247-254.
[8]. CRYPTREC, Cryptographic Technology Guideline (Lightweight Cryptography), 2017.
[9]. Dhanabal, L & Shantharajah, SP 2015, "A Study on NSL-KDD Dataset for Intrusion Detection System Based on Classification Algorithms", International Journal of Advanced Research in Computer and Communication Engineering, vol. 4, no. 6, pp. 446- 452.
[10]. 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.
[11]. Isha & Luhach, AK 2016, "Analysis of Lightweight Cryptographic Solutions for Internet of Things", Indian Journal of Science and Technology, vol. 9, no. 28, pp. 1-7.
[12]. McKay, KA, Bassham, LE, Turan, MS & Mouha, NW 2017, "Report on Lightweight Cryptography", National Institute of Standards and Technology, pp. 1-27.
[13]. Roshan, S, Miche, Y, Akusok, A & Lendasse, A 2018, "Adaptive and online network intrusion detection system using clustering and Extreme Learning Machines", Journal of the Franklin Institute, vol. 355, no. 4, pp. 1752-1779.
[14]. C. Wei, "Application of data encryption technology in computer network security", Journal of Physics: Conference Series, vol. 1237, no. 23, Article ID 022049, 2019.
[15] A. Sultan, X. Yang, and A. A. E. Hajomer, "Chaotic constellation mapping for physical-layer data encryption in OFDM-PON", IEEE Photonics Technology Letters, vol. 99, no. 4, p. 1, 2018.
[16] Y. Zhang, W. Yang, and Z. Zhang, "Application strategy of data encryption technology in computer network security", Electronics Research and Applications, vol. 2, no. 5, pp. 4–10, 2018.
[17] Y. Shi, "Research on implementation method of key management based on data encryption technology," IOP Conference Series: Materials Science and Engineering, vol. 677, no. 4, Article ID 042018, 2019.
[18]. Chen, J.J.; Yan, D.W.; Duan, S.K.; Wang, L.D. Memristor-based hyper-chaotic circuit for image encryption. Chin. Phys. 2020, 29, 110504.
[19]. Liu, H.; Zhao, B.; Huang, L. Quantum image encryption scheme using Arnold transform and S-box scrambling. Entropy 2019, 21, 343.
[20]. Awaad, M.H.; Jebbar, W.A. Prolong the lifetime of WSN by determining a correlation nodes in the same zone and searching for the best not the closest CH. Int. J. Mod. Educ. Comput. Sci. 2014, 6, 31.
[21]. Arfat Ahmad Khan, Khalid K. Almuzaini, Víctor Daniel Jiménez Macedo, Stephen Ojo, Vinodh Kumar Minchula, Vandana Roy, MaReSPS for energy efficient spectral precoding technique in large scale MIMO-OFDM, Physical Communication, Volume 58, 2023, 102057, ISSN 1874-4907, https://doi.org/10.1016/j.phycom.2023.102057.
[23]. Sadhya, D.; Sing, S.K. Providing robust security measures to bloom filter based biometric template protection schemes. Comput. Secur. 2017, 67, 59–72.
[24]. Lim, K.; Liu, W.; Wang, X.; Joung, J. SSKM: Scalable and secure key management scheme for group signature based authentication and CRL in VANET. Electronics 2019, 8, 1330.
[25]. Sampangi, R.V.; Sampalli, S. Metamorphic framework for key management and authentication in resource-constrained wireless networks. Int. J. Netw. Secur. 2017, 19, 430–442.
[26]. Al-Zubaidie, M.; Zhang, Z.; Zhang, J. RAMHU: A new robust lightweight scheme for mutual users authentication in healthcare applications. Secur. Commun. Netw. 2019, 2019, 3263902.
[27]. Al-Zubaidie, M.; Zhang, Z.; Zhang, J. PAX: Using pseudonymization and anonymization to protect patients' identities and data in the healthcare system. Int. J. Environ. Res. Public Health 2019, 16, 1490.
[28]. Parmod Kumar, Anupam Baliyan, K. Ramalingeswara Prasad, N. Sreekanth, Parag Jawarkar, Vandana Roy, Enoch Tetteh Amoatey, "Machine Learning Enabled Techniques for Protecting Wireless Sensor Networks by Estimating Attack Prevalence and Device Deployment Strategy for 5G Networks", Wireless

Doi : https://doi.org/10.54216/JCIM.120102
Received: December 04, 2022 Revised: January 20, 2023 Accepted: April 20, 2023

Communications and Mobile Computing, vol. 2022, Article ID 5713092, 15 pages, 2022. https://doi.org/10.1155/2022/5713092.

[29]. Zhang, Y.; Pengfei, J. An efficient and hybrid key management for heterogeneous wireless sensor networks. In Proceedings of the 26th Chinese Control and Decision Conference (2014 CCDC), Changsha, China, 31 May 2014–2 June 2014; pp. 1881–1885.

Doi : https://doi.org/10.54216/JCIM.120102
Received: December 04, 2022 Revised: January 20, 2023 Accepted: April 20, 2023