A Concentrated Energy Consumption Wireless Sensor Network by Symmetric Encryption and Attribute Based Encryption Technique

Anita Soni
CSE Department, IES University Bhopal, India
Email: anita.soni@iesuniversity.ac.in

Abstract

Wireless sensor networks (WSNs) are increasingly used in a wide variety of settings, including defence, industry, healthcare, and education. 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 BS then sends the data out to the users over the internet. The sensor network's adaptability, portability, dependability, and quickness are driving its widespread use across industries. The suggested SHS evaluates the efficiency of well-established symmetric algorithms to see where it stands in the spectrum of security. The Blowfish encryption algorithm was proven to require the least amount of processing power after extensive benchmarking. Therefore, the Blowfish algorithm is selected to protect sensitive medical information. The medical database receives the encrypted health records. Only those with proper permissions should be able to access them. Therefore, the CP-ABE is implemented to regulate access to patient records. The SHS's results on the dataset are compared to those of other existing systems. With SHS, health data may be transmitted to doctors rapidly and securely because it requires less computing time and energy. In addition to these benefits, SHS also offers privacy, authentication, and authorization.

Keywords: Encryption; Symmetric Encryption; WSN; Energy Consumption

1. Introduction:

Fitness observing, military investigation, manufacturing observing, mudslide recognition, and so on are all examples of open and sensitive environments ideal for WSN deployment. There are two primary kinds of nodes in it: 1) Sensor nodes, and 2) Sink nodes. The sensor nodes resemble minicomputers in many ways, although they are significantly less powerful and have shorter battery lives [1]. When data is gathered and processed centrally, it all ends up at the sink node, also known as the base station (BS). Aggregators (cluster heads) are often the most powerful sensor nodes, but normal nodes can also play this role. These aggregators compile and analyse information from the network's various sensors. Calculating temperatures, for instance, can benefit from the application of aggregation operations such as sum, min, and max. The aggregator takes in information from multiple sensors, adds up the results, and sends the final tally on to the sink node [2]. By reducing the number of data transfers between nodes, the lifetime of the network is extended.

When data is aggregated, it means that information is pooled from a number of different sensor nodes and then delivered to the BS in the appropriate format. Either new data will be injected into the network, or the aggregation will fail due to the compromised node's influence. The currently available techniques do not offer a cohesive solution to the challenge of data aggregation that is both energy-efficient and secure [3]. Complex security algorithms require a greater amount of electricity from each sensor node, which reduces the overall lifespan of the network. The application of WSN in the field of health monitoring systems is particularly fruitful. The disclosure of confidential material can result in personal and professional repercussions as well as legal difficulties.

Doi : https://doi.org/10.54216/JCIM.120101
Received: November 25, 2022 Revised: January 25, 2023 Accepted: March 18, 2023

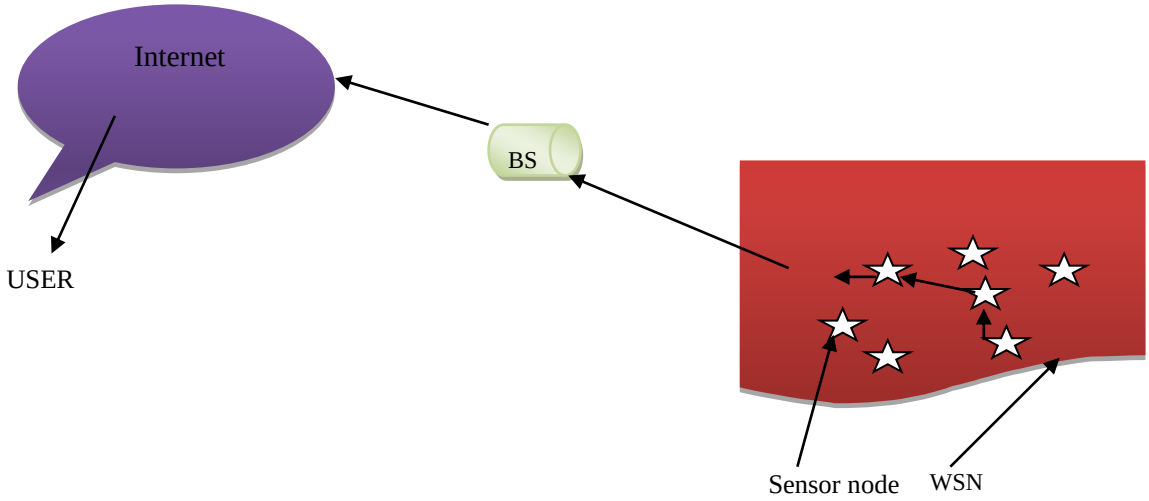

Figure 1: Architecture of Sensor Node.

An intrusion detection system is one of the top-tier security mechanisms in WSN. This system can identify potential dangers that were missed by the preventive system. The vast majority of solutions for intrusion detection systems (IDS) exclusively search for threats on the network layer and ignore other layers [4].

The military uses sensor networks for a variety of objectives, some of which include border surveillance, soldier tracking and threat recognition, identifying enemy movements, discovering land mines, discovering unmanned surveillance vehicles, discovering forest fires, and other similar activities. As a consequence of this, the utilisation of sensor networks within the defence industry enables the quick transfer of urgent information to the BS [5].

The use of sensor networks allows for the tracking of the health of sportsmen as well as the elderly, both of whom require continuous monitoring. Patients would see an improvement in their quality of life in addition to financial savings brought about by sensor-based health monitoring. The incorporation of sensor networks into production facilities makes it possible to do continuous inspections of machinery, hence reducing the amount of time that workers need to spend doing so [6]. With the assistance of the sensor network, one is able to monitor a wide variety of factors, including but not limited to temperature, humidity, water content, pollution, fire, smoke, detection of landslides, and so on. When we talk about keeping sensitive information hidden from prying eyes while it is being transmitted by sensor networks, we are referring to the concept of data confidentiality. In two circumstances, it is required that it be guaranteed:

i) The sensor data are private and confidential; hence, they should only be accessible to approved users.

ii) In order to prevent traffic analysis attacks, it is necessary to encrypt sensitive data such as sensor identities and public keys.

The term "data integrity" refers to the certainty that the data received from the sender has not been tampered with in any way [7]. There are two possible causes of tampered sensor data:

i) Unofficialoperatorsinterferingthrough the statistics

ii) Information may be lost due to the extreme conditions.

2. Related Work

The authors utilised a method called as efficient provably secure aggregation of encrypted data in WSN so that they could accomplish their goal. An additive homomorphic cryptosystem was utilised in order to encrypt the data. The checksum ensures that the message has not been altered in any way, and the header provides a list of the IDs of all of the reporting nodes. The sink node receives all three values. In order to protect themselves from the node exclusion attack, all of the nodes in the network generate a Message Authentication Code tag for their HDR. The high-dimensional result will be accepted by the sink [8] if the result is consistent with the tag. The strength of the method is based on the fact that the keys are created with

Doi : https://doi.org/10.54216/JCIM.120101
Received: November 25, 2022 Revised: January 25, 2023 Accepted: March 18, 2023

the assistance of a completely untraceable pseudorandom generator. However, the approach does have a few drawbacks, such as the fact that it is less secure against internal assaults and that the calculation cost rises as a result of the usage of Message Authentication Code (hdr) [9-11]. These are just two of the limits of the method.

Secure End-to-End Data aggregate, also known as SEEDA, is a protocol that utilises additive homomorphic encryption to ensure the safety of data aggregate. At each node, the message is first encrypted utilising a private key, and then it is transmitted to the h-1 nodes that are above them [12]. The information that has been compiled is transmitted to the h-2 level of nodes, together with a count value that indicates the number of nodes that did not react. Following the encrypting of the count value, the sink node will next proceed to decode the message in order to calculate an average. It is an upgrade over the methods that came before it because it utilises the most advantageous aspects of both hop-by-hop encryption and end-to-end encryption. The method has the issue that it does not take into consideration any verification mechanism to demonstrate data authentication [13-15]. This is a significant limitation of the method.

Recent developments in WSN have spawned a wide variety of application domains relating to healthcare, which has resulted in an overall improvement in the standard of living for humans. It was the impetus for the development of the field of WMSN. It is possible to monitor and keep track of human health using any of the existing biosensor devices, regardless of whether or not the devices are worn. The use of WMSN can be beneficial for athletes as well as patients who require continuous monitoring either at a medical facility or at home [16-18]. The data from the biosensors are then transmitted to the medical facility over the wireless network so that it may be analysed. When it comes to the transmission of sensitive health information, wireless networks provide a potential security issue. There is a possibility that the information on the person will be mismanaged while it is being transmitted, which could put their life in danger. As a consequence of this, privacy and security need to be given top priority in healthcare applications [19-22].

The authors have utilised a two-pronged strategy in order to detect attacks in the network that involve the dropping of packets and the injection of counterfeit packets. To begin, measures that are based on thresholds are used to identify behaviour that is not typical. In conjunction with the threshold technique [23-25], the use of characteristics of traffic that include the packet reception rate and the packet inter arrival time are encouraged. In the second stage, you will identify whether or not an assault is currently taking place by employing a fuzzy inference method. The strategy is implemented on the network's neighbours that are accessible through a single hop. If the node discovers that one of its neighbours is being targeted by an adversary, it will remove that neighbour from its list of neighbours and send an alert to the BS [26].

Researchers have suggested developing intrusion prevention and detection systems for use in commercial settings. The Intrusion Prevention System (IPS) is responsible for the provision of the data, the authentication of the nodes, and the prevention of eavesdropping. The intrusion detection system (IDS) is a secondary line of defence that is intended to stop any attacks on the network that the intrusion prevention system (IPS) missed [27]. In addition to this, we employ physical motes to highlight the significance of one-hop clustering and give a hierarchical framework for detecting additional attacks. This is done by analysing the relationships between the motes.

At the physical, MAC, and network layers of the system, the investigators have placed agents that are capable of recognising any breaches that may have occurred. When an unauthorised node in the network receives a request to send a frame, the detection system uses two separate methods to verify the request's legitimacy: i) the node's availability in the routing table to ensure that the Request to Send frame was sent by a trusted neighbour, and ii) the received signal strength indicator value [28]. Both of these methods are used to ensure that the Request to Send frame was sent by a trusted neighbour. These two approaches are utilised in tandem to confirm that the Request to Send frame was transmitted by a reliable neighbour. An innovative solution to the challenge of detecting cross-layer attacks, such as the hello flood attack, the cloning attack, and the sink hole attack, has been developed by the intrusion detection system (IDS). The most significant benefit of the system is that it only needs a single detection system to be able to detect assaults on numerous layers, which eliminates the requirement of designing separate IDS for each layer [29]. This is the most significant benefit of the system.

The authors suggest an intrusion detection and prevention system suitable for use in manufacturing settings. The data, node authentication, and eavesdropping prevention are all provided by the Intrusion Prevention System (IPS). The IDS is a secondary layer of defence meant to prevent any attacks on the network that the IPS missed. Furthermore, a hierarchical framework is proposed for detecting the other attacks, and real motes are used to demonstrate the significance of the one-hop grouping.

Doi : https://doi.org/10.54216/JCIM.120101
Received: November 25, 2022 Revised: January 25, 2023 Accepted: March 18, 2023

Additionally, studies have reported that there are three stages to the Hybrid IDS. A rule-based anomaly detection model initially eliminates information that doesn't fit the norm. The second phase involves sending the filtered aberrant data to a misuse detection model, which then classifies the data based on known attacks to remove them. After the anomaly detection model and the misuse detection model have combined their findings, the rule based decision making model may identify the attacks and the specific type of attack, and then notify the administrator. The scheme's benefit is that it saves energy by just sending filtered data to the abuse detection model and by speeding up decision making thanks to rules in the model.

It has been noted in the literature that a central agent employs decision tree approaches at the BS, whereas a local agent makes use of threshold-based metrics at the mote. The local agent will alert the main agent if it notices something out of the ordinary. 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 use of the centralised agent.

Researchers have taken a similar two-pronged approach to detecting assaults that involve the discarding of packets or the injection of bogus packets into the network. First, threshold-based measurements identify the out-of-the-ordinary activity. Attributes of traffic such as packet reception rate and packet inter arrival time are used in conjunction with the threshold technique. The second stage involves using a fuzzy inference method to determine if an attack is in progress. The approach is deployed to the network's one-hop neighbours. In the event of an attack, the node will report the offending node to the BS and remove it from the neighbouring list.

3. The Proposed Work

It may be necessary to connect one or more sensors to a patient's body in order to properly diagnose their condition. These sensors may include a heart rate monitor, a blood pressure monitor, an electrocardiogram sensor, or a body temperature sensor. Before it is sent, the information gathered by the sensors is encrypted on the central controller unit (the mobile phone) using the Blowfish algorithm. The sensitive nature of the data that healthcare apps manage requires them to conform to the highest possible standards of encryption. There would be a wide variety of user types that could access the medical information. Other users, such as family members and patients, need access to only certain elements of the record. However, in the event of an emergency, medical professionals require access to the entirety of a patient's medical record. A breach of confidentiality involving highly confidential medical information could have lethal repercussions. It is of the utmost importance to maintain strict control over who can view private patient information. Through the use of access control, individuals' employment determine the permissions that are granted to them.

Cryptographic mechanisms are used to control who has access to the data. A collection of users who collectively possess expressive capabilities in order to produce an access key that may be utilised as a secret. When it comes to methods of access control that are based on cryptography, medical and military applications typically make use of something called attribute-based encryption, or ABE for short.

The components of ABE systems might vary from one another in a variety of ways. ABE systems can be divided into four primary categories: those that use threshold-policy access control, those that use key-policy access control, those that use cypher text-policy access control, and those that use non-monotonic policy access control. Control of access to encrypted text that is determined by policy. For each of the qualities in the cypher text policy, there is a key that corresponds to a certain access structure. The freedom of the owner of the data to determine who can decrypt the encrypted data is enhanced. This flexibility was previously limited. The policy provides for a greater degree of flexibility with regard to the modification of the access model. As a consequence, the ABE cypher text policy has been put into effect at SHS.

The information can be transmitted in an encrypted form to the diagnostic centre via either Wi-Fi or 3G. This central location is responsible for storing and processing all of the data that was gathered by the sensors. When a patient visits a diagnostic centre, the information they provide can be entered into a database, which can then be used to monitor the patient's health over time. Using the CP-ABE approach, authorised members of the medical community, such as physicians, nurses, and technicians, are able to access patient records. When a patient's condition is life-threatening, the helicopter ambulance can use GPS to locate the patient's precise location and fly straight to them. An illustration of the proposed system is provided for our perusal in Figure 2.

Doi : https://doi.org/10.54216/JCIM.120101
Received: November 25, 2022 Revised: January 25, 2023 Accepted: March 18, 2023

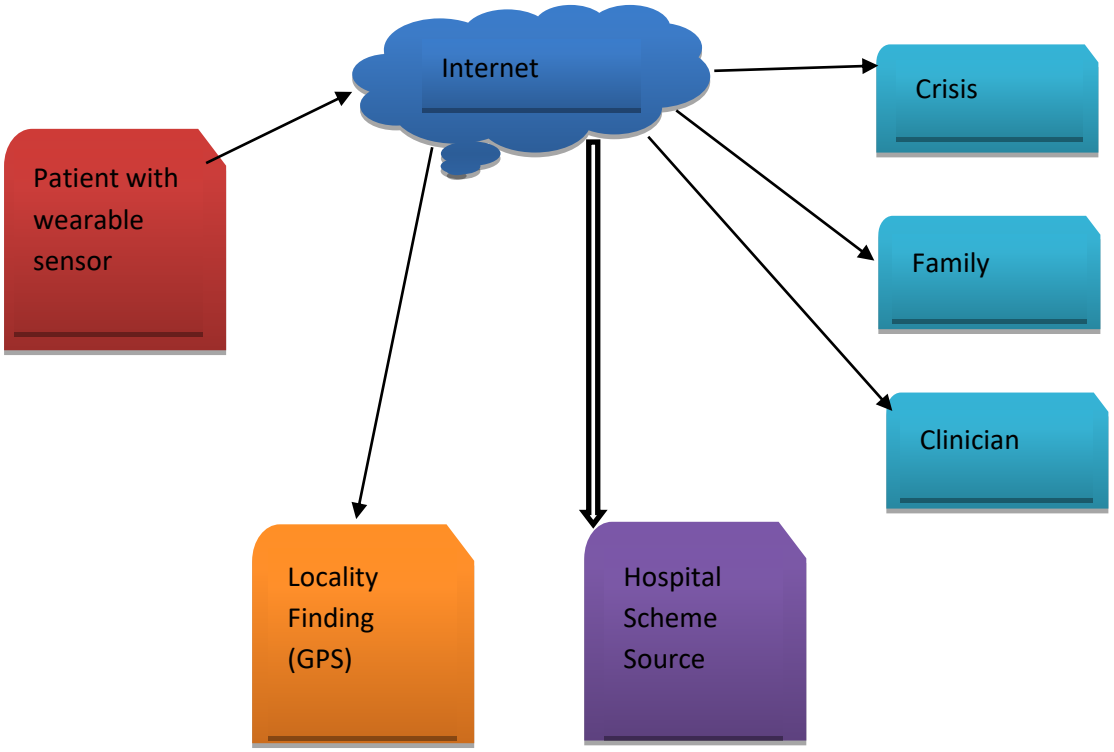

Figure 2: The Projected System Model.

3.1. Blowfish technique:

Medical records are encrypted using the Blowfish technique in the current study, and only the encrypted records are sent to the diagnostic facility. Key sizes in the Blowfish algorithm range from 32 bits to 448 bits, while the block size is 64 bits. This Feistel cipher has 16 rounds and makes use of big key-dependent S-boxes. The F-function takes a 32-bit input and splits it into four eight-bit halves that are then fed into the S-boxes. The S-boxes take 8-bit data as input and output 32-bit data. This process is recurringtill the wantedresult is attained. After round 16, there is a reversal of the final swap, and by round 18, you will be able to XOR R with K17 and L with K18. The processes involved in decryption are identical to those involved in encryption; the only difference is that the order of the prime integers P1, P2,..., P18 is switched around. The gradient appearance is defined as:

$$\nabla f(X) = H_c^{\top}(H_c X H_r - Y)H_r^{\top} \quad (1)$$

Eq. (2) expressed in following form

$$X^{l+1} = P_v(X^l - \eta H_c^{\top} H_c X^l H_r H_r^{\top} + C) \quad (2)$$

Initiation function ψ is well-defined as a linedgrouping of K DoG and lined function is demarcated in equation 3 and 4.

$$\psi(u) = \sum_{k=1}^{K} P\, c_k \phi_k(u), u \in R, \quad (3)$$

Where,

$$\phi_k(u) = u exp\left(-\frac{(k-1)u^2}{2\tau^2}\right) \quad (4)$$

Doi : https://doi.org/10.54216/JCIM.120101
Received: November 25, 2022 Revised: January 25, 2023 Accepted: March 18, 2023

The data D comprises N instances$\{(Y_q, X_q)\}_{q=1}^{N}$, where $Y_q = H_c X_q H_r^{\top} + \xi_{q^*}$Arbitrary vectors ξ_q are measured to be correspondinglydisseminated as well as sovereign. Let $c^l \in R^K, l = 1$ be measurements. By plummeting squared approximation error over altogether training instances, optimum set of initiationstipulations c* is attained (5)

$$J(c) = \frac{1}{2}\sum_{q=1}^{N} \| X_q^L(Y_q, c) - X_q \|_2^2 \quad (5)$$

Incline of J(c) with deference to c is mandatory for optimization. If a very miniature step size is quantified, optimization of J(c) applying vanilla GD inclines to deviate.

CP-ABE: Many people, including loved ones, medical staff, and hospital staff, would need access to patient information. To ensure that only authorized personnel have access to sensitive patient information, the diagnostic centre uses cipher text-policy access control.

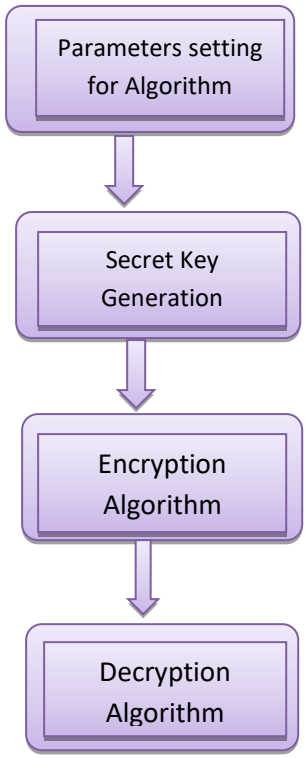

Figure 3: The CP-ABE algorithm flow-chart.

Public key parameters, an access structure, and a message are encrypted using the cipher text policy. Each user's private key has its own unique collection of attributes that signify the user's level of access. The message is encrypted so that only those users with the necessary qualities can read it. When creating a secret key in SHS, the patient id is one of the attributes used. There are four stages to the CP-ABE algorithm.

i). Secret key and authentication key is created.

ii). The message M, the entréearrangement A over the creation of characteristics, and the public parameters MPK are the inputs to the encryption algorithm, which generates a cipher text CT related to the attribute set as the output.

iii). Similarly, the decryption method requires three inputs before it can produce a message: the public parameter MPK, the cipher text CT linked to the access structure A, and the private key SK with the attribute set S. The procedure will produce an empty set if S does not conform to the access structure.

The SHS technique is secure against dictionary attacks, brute force assaults, and collusion attacks since it combines the blowfish encryption algorithm with ABE.

Doi : https://doi.org/10.54216/JCIM.120101
Received: November 25, 2022 Revised: January 25, 2023 Accepted: March 18, 2023

4. Results

When compared to their asymmetric counterparts, symmetric key algorithms are superior in terms of key size, memory requirements, and computational time. Since the intended recipients of the medical information are likely to be limited to a small group, including the patient's doctor, nurse, technician, and possibly some family members, the adoption of symmetric key methods makes sense. In SHS, symmetric algorithms are deemed to be the most appropriate algorithms for protecting the confidentiality of patient information. In asymmetric key algorithms, the encryption and decryption keys are different, but in symmetric key encryption they are the same. There are two subcategories of symmetric key algorithms: stream ciphers and block ciphers. Stream ciphers typically encrypt data bit by bit, using separate keys for each encrypted byte. The blocks of data or files (often between 64 and 128 bits in length) are encrypted using block ciphers with the same key. After the patient has been observed for a set amount of time, a block or file containing their health records is sent to the hospital. In SHS, a symmetric block cipher is used to encrypt sensitive medical information.

The SHS algorithm is deployed in the computer system via the dataset and the Net Beans IDE. Encryption time, decryption time, and total calculation time are used to evaluate algorithm performance.

Table 1: Scheming of Encryption time for various file sizes.

Methodology	**Size of the File**				
	50 kB	**200 kB**	**400 kB**	**1000 kB**	**3000 kB**
Advanced Encryption Standard (AES) and Message Digest 5 (s)	1	2.3	3.6	9.2	12.4
CP -ABE and Advanced Encryption Standard (s)	3.4	4.6	6.7	12.5	14.6
Blowfish and CP-ABE (s) -SHS	0.9	1	2.4	7.5	8.6

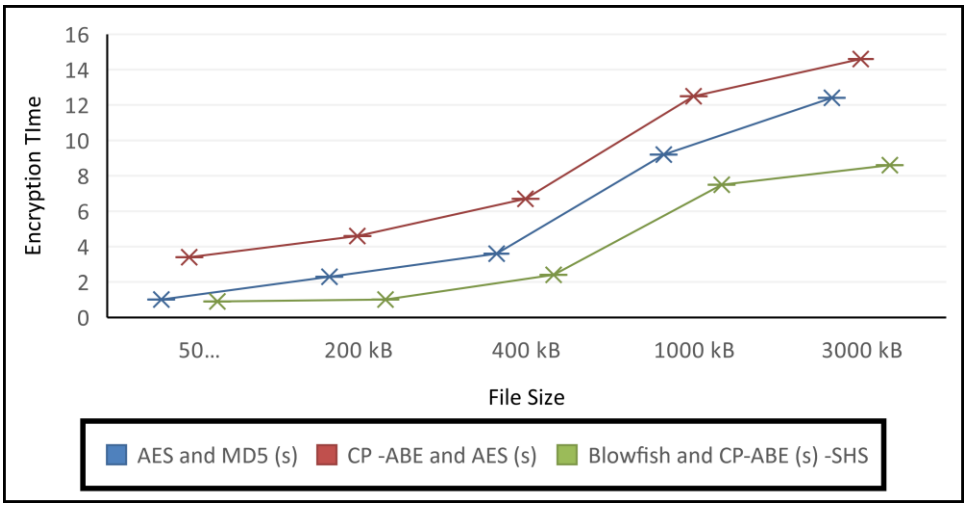

Figure 3: Scheming of Encryption time for various file sizes.

Doi : https://doi.org/10.54216/JCIM.120101
Received: November 25, 2022 Revised: January 25, 2023 Accepted: March 18, 2023

The encryption times for the various algorithm mixtures are shown in Table 1 and Figure 3. From table 1 and Figure 3, it can be concluded that, encryption time of the proposed algorithm the combination of Blowfish and CP-ABE is least among the all-existing algorithms. Which proves the success of the proposed algorithm.

Table 2: Scheming of Decryption time for various file sizes.

Methodology	**Size of the File**				
	50 kB	**200 kB**	**400 kB**	**1000 kB**	**3000 kB**
Advanced Encryption Standard (AES) and Message Digest 5 (s)	4.2	5.4	7.6	8.9	11.2
CP -ABE and Advanced Encryption Standard (s)	7.4	8.6	10.8	13.2	14.6
Blowfish and CP-ABE (s) -SHS	2.2	3.5	4.3	6	6.2

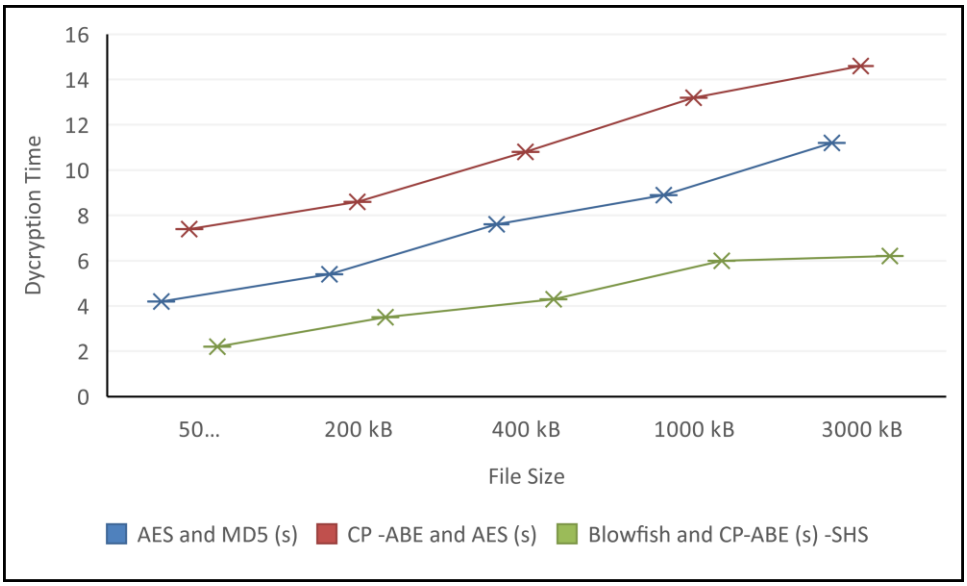

Figure 4: Scheming of Decryption time for variousfile sizes.

The decryption times for all algorithm combinations are displayed in table 2 and figure 3, respectively. The Decryption time of the proposed algorithm the combination of Blowfish and CP-ABE is least among the all-existing algorithms. Which proves the success of the proposed algorithm.

Since the session key must be encrypted and decrypted prior to the encryption and decryption of actual messages, CP-ABE and AES have much longer encryption and decryption times than AES and MD5. When compared to the AES and MD5 algorithms, this one is very resource intensive.

Doi : https://doi.org/10.54216/JCIM.120101
Received: November 25, 2022 Revised: January 25, 2023 Accepted: March 18, 2023

Table 3: Computationof Whole Calculation time for various file sizes.

Methodology	Size of the File				
	50 kB	**200 kB**	**400 kB**	**1000 kB**	**3000 kB**
Advanced Encryption Standard (AES) and Message Digest 5 (s)	8.6	10.7	15.9	20.7	24.8
CP -ABE and Advanced Encryption Standard (s)	11.6	13.8	17.6	28.9	32.7
Blowfish and CP-ABE (s) - SHS	5.2	7.5	8.3	12.7	14.8

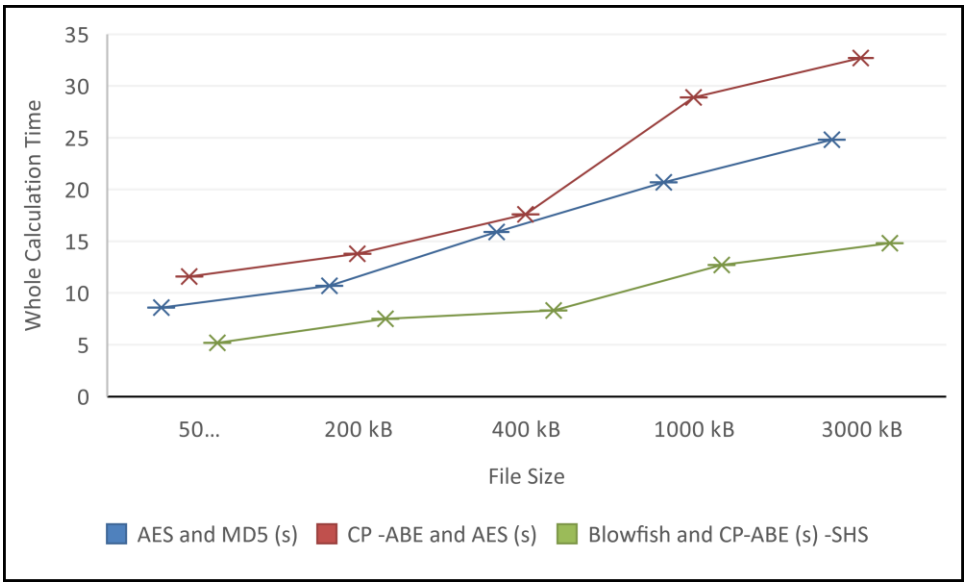

Figure 5: Computation of Whole Calculation time for various file sizes.

The sum of each algorithm's processing time is displayed in table 3 and graph 5. When compared to other algorithms, the computation time required by SHS's use of Blowfish and CP-ABE is negligible. The medical information must swiftly reach its intended recipients, including physicians and other healthcare professionals. The Blowfish algorithm is superior to any other combination of algorithms because it requires so little processing time. Users also receive access control via the CP-ABE algorithm's execution. SHS uses a combination of the Blowfish and CP-ABE algorithms to ensure the privacy and security of sensitive medical information.

5. Conclusion

The sensor nodes of a WSN report back to the BS any changes they detect in their surrounding physical environment. In order to cut down on communication expenses, power consumption, and redundant data,

Doi : https://doi.org/10.54216/JCIM.120101
Received: November 25, 2022 Revised: January 25, 2023 Accepted: March 18, 2023

sensor networks aggregate collected information. Since adversaries can easily target sensor data, securing sensor data is a crucial area of study. While numerous security methods have advanced, few have made strides toward significantly reducing energy consumption. The amount of power a network uses is directly related to the amount of time it takes to calculate security algorithms. Data integrity, confidentiality, and authenticity are just few of the security qualities prioritized by the offered security approaches. One of the most important uses of WSN is in remote health monitoring systems. Patient situations would become more complicated if health information was mishandled or delayed. Fast and secure transmission of the tracked health information to hospitals and clinicians is essential. The best symmetric algorithm and access control methods are therefore investigated. The gender, temperature, and pulse rate parameters are used to determine whether Blowfish or CP-ABE should be used. Research into lightweight symmetric algorithms is conducted to drastically cut the processing time for low powered devices. In the end, Speck and CP-ABE are combined and used on health records.

Funding: "This research received no external funding"

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

References

[1]. Alemdar, H &Ersoy, C 2010, „Wireless sensor networks for healthcare: A Survey", Computer Networks, vol. 54, no. 15, pp. 2688-2710.
[2]. Alkhatib, AAA &Baicher, GS 2012, „Wireless Sensor Network Architecture", Proceedings of International Conference on Computer Networks and Communication Systems, pp. 11-15.
[3]. Alonso, JV, Matencio, PL, Castano, FJG, Hellin, HN, Guirao, PJB, Martinez, FJP, Alvarez, RPM, Jimenez, DG, Castineira, FG & Fernandez, RD 2010, „Ambient Intelligence Systems for Personalized Sport Training", Sensors, vol. 10, no. 3, pp. 2359-2385.
[4]. Alrajeh, NA, Khan, S & Shams, B 2013, „Intrusion Detection System in Wireless Sensor Networks", International Journal of Distributed Sensor Networks, pp. 1-7.
[5]. Doshi, N &Jinwala, D 2012, Constant Ciphertext Length in CP-ABE, IACR Cryptology ePrint Archive.
[6]. Duche, RN &Sarwade, NP 2014, „Sensor Node Failure Detection Based on Round Trip Delay and Paths in WSNs", IEEE Sensors Journal, vol. 14, no. 2, pp. 455-464.
[7]. Parmod Kumar, AnupamBaliyan, K. Ramalingeswara Prasad, N. Sreekanth, Parag Jawarkar, Vandana Roy, Enoch TettehAmoatey, "Machine Learning Enabled Techniques for Protecting Wireless Sensor Networks by Estimating Attack Prevalence and Device Deployment Strategy for 5G Networks", Wireless Communications and Mobile Computing, vol. 2022, Article ID 5713092, 15 pages, 2022. https://doi.org/10.1155/2022/5713092.
[8]. McKay, KA, Bassham, LE, Turan, MS &Mouha, NW 2017, „Report on Lightweight Cryptography", National Institute of Standards and Technology, pp. 1-27.
[9]. 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.
[10]. Raja Rajeswari, S &Seenivasagam, V 2016, „Comparative Study on Various Authentication Protocols in Wireless Sensor Networks", The Scientific World Journal, vol. 2016.
[11]. Rekha, R, GayathriMathambigai, T &Vidhyapriya, R 2012, „Secure Medical Data Transmission in Body Area Sensor Networks Using Dynamic Biometrics and Steganography", Bonfring International Journal of Software Engineering and Soft Computing vol. 2, no. 1, pp. 5-11.
[12]. 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.
[13]. C. Wei, "Application of data encryption technology in computer network security," Journal of Physics: Conference Series, vol. 1237, no. 23, Article ID 022049, 2019.
[14] 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.
[15] 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.
[16] 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.

Doi : https://doi.org/10.54216/JCIM.120101
Received: November 25, 2022 Revised: January 25, 2023 Accepted: March 18, 2023

[17]. Idrees, B.; Zafar, S.; Rashid, T.; Gao, W. Image encryption algorithm using S-box and dynamic Hénon bit level permutation. Multimed. Tools Appl. 2020, 79, 6135–6162.
[18]. Liu, H.; Zhao, B.; Huang, L. Quantum image encryption scheme using Arnold transform and S-box scrambling. Entropy 2019, 21, 343.
[19]. Rehman, A.U.; Firdous, A.; Iqbal, S.; Abbas, Z.; Shahid, M.M.A.; Wang, H.; Ullah, F. A Color Image Encryption Algorithm Based on One Time Key, Chaos Theory, and Concept of Rotor Machine. IEEE Access 2020, 8, 172275–172295.
[20]. S. Bera, S. Misra, S. Kumar Roy, and M. S. Obaidat, "Soft-WSN: software-defined WSN management system for IoT applications," IEEE Systems Journal, vol. 12, no. 3, pp. 2074–2081, 2016.
[21]. A. N. Alvi, S. H. Bouk, S. H. Ahmed, M. A. Yaqub, M. Sarka, and H. Song, "BEST-MAC: bitmap-assisted efficient and scalable TDMA based WSN MAC protocol for smart cities," IEEE Access, vol. 4, no. 1, pp. 312–322, 2016.
[22]. X. Yuan, M. Elhoseny, H. K. E-Minir, and A. M. Riad, "A genetic algorithm-based, dynamic clustering method towards improved WSN longevity," Journal of Network and Systems Management, vol. 25, no. 1, pp. 1–26, 2016.
[23]. C. Zhang, T. Xie, K. Yang et al., "Positioning optimisation based on particle quality prediction in wireless sensor networks," IET Networks, vol. 8, no. 2, pp. 107–113, 2019.
[24]. V. Bapat, P. Kale, V. Shinde, N. Deshpande, and A. Shaligram, "WSN application for crop protection to divert animal intrusions in the agricultural land," Computers and Electronics in Agriculture, vol. 133, pp. 88–96, 2017.
[25]. H. Grichi, O. Mosbahi, M. Khalgui, and Z. Li, "RWiN: new methodology for the development of reconfigurable WSN," IEEE Transactions on Automation Science and Engineering, vol. 14, no. 1, pp. 109–125, 2017.
[26]. Y. He, Z. Zhang, F. R. Yu et al., "Deep reinforcement learning-based optimization for cache-enabled opportunistic interference alignment wireless networks," IEEE Transactions on Vehicular Technology, vol. 66, no. 11, pp. 10433–10445, 2017.
[27]. Y. He, N. Zhao, and H. Yin, "Integrated networking, caching, and computing for connected vehicles: a deep reinforcement learning approach," IEEE Transactions on Vehicular Technology, vol. 67, no. 1, pp. 44–55, 2018.
[28]. H. Mostafaei, M. U. Chowdhury, and M. S. Obaidat, "Border surveillance with WSN systems in a distributed manner," IEEE Systems Journal, vol. 8, no. 4, pp. 1–10, 2018.
[29]. N. E. Rachkidy, A. Guitton, and M. Misson, "Avoiding routing loops in a multi-stack WSN," Journal of Communications, vol. 8, no. 3, pp. 151–160, 2018.

Doi : https://doi.org/10.54216/JCIM.120101
Received: November 25, 2022 Revised: January 25, 2023 Accepted: March 18, 2023