Lightweight Symmetric Encryption and Attribute Based Encryption Method to Increase Information Safety in Wireless Sensor Network

Rajeev Pandey

University Institute of Technology RGPV, Bhopal, India

Email: rajeevpandey@rgpv.ac.in

Abstract

Direct data transmission in a wireless sensor network raises the data transfer cost. 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. The sensor nodes and their collected data are vulnerable to destruction because they are broadcasting in a hostile environment. Therefore, data security is a major topic of study for WSN. Due to the limited resources of the sensor network, conventional wireless network security measures are ineffective. With Speck encryption and CP-ABE, the proposed Lightweight Secured remote Health monitoring System (LSHS) can protect health data and restrict who can access it while using less power. Lightweight block ciphers are optimal for protecting medical records, according to the research. Using the LSHS, we evaluate how well-known lightweight block ciphers like AES, Simon, and Speck perform. Both encrypting and decrypting with the Speck technique require less processing time. Therefore, medical records are encrypted using the Speck algorithm.

Keywords: CP-ABE; LSHS; WSN; Encryption.

1. Introduction:

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. Information is sent out to users from the BS via the internet. The sensor network's adaptability, portability, durability, and reactivity make it a prime candidate for usage in a wide variety of applications [1].

The ADC receives data from the sensors about the surrounding environment, including the temperature, light, humidity, pressure, and so on. The ADC (analog-to-digital converter) 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 [2]. The power component is the utmost critical portion of a sensor node because it provides juice to everything else. 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 [3]. Turning off the transceiver while it's not in use helps save electricity. It also features a locator, a mobilizer, and a power generator, all of which can be activated depending on the situation. In order to transmit data, it is necessary to determine the location of the sensor nodes that have been deployed. Using the mobilizer device, the sensor nodes can be relocated to a new area [4].

Doi: https://doi.org/10.54216/JCIM.100205
Received: May 15, 2022 Accepted: August 18, 2022

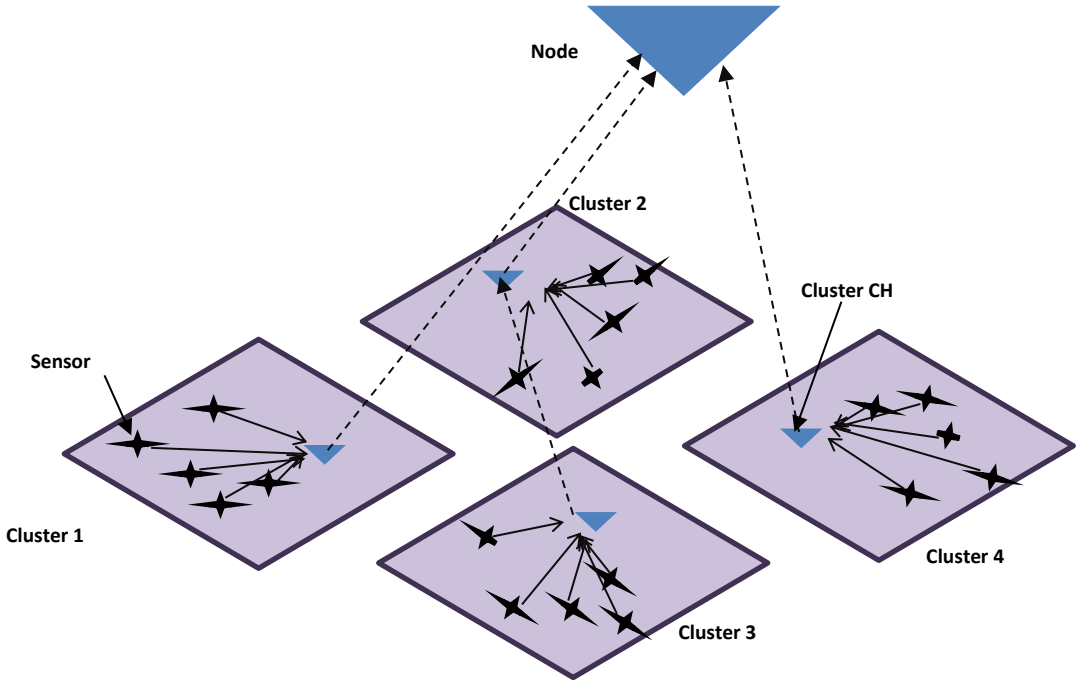

Figure 1: Wireless sensor node clustering.

All of the sensor nodes agree on the same set of keys so that their data may be transmitted safely. They prevent unwanted devices from connecting to the network and exchanging data. They can accommodate a large number of sensor nodes, sometimes in the thousands. Spoofing attacks, replaying routing information, and selective forwarding are all possible with the current wireless network routing technologies [5]. Therefore, it is difficult to design a secure routing protocol for WSN. The sensor nodes can be easily compromised by physical means of assault. Capturing sensor nodes can provide attackers access to cryptographic keys and allow them to alter the code. Strengthening resistance to node capture attacks is a challenging endeavour. In order to save power, the cluster head collects all of the detected data and sends it to either the next-level cluster head or the BS [6]. The data collection could be abandoned by the attackers. As a result, protecting data aggregation is crucial in WSN [7].

When data is aggregated, it is combined from multiple sensor nodes and sent to the BS in the proper format. The compromised node might either inject new data into the network or cause the aggregation to fail [8]. The current methods do not provide a unified answer to the problem of energy-efficient and safe data aggregation. Complex security algorithms require more power from each sensor node, shortening the lifespan of the network as a whole. WSN is especially useful in the realm of health For secure data transmission, each sensor node uses the same set of keys. They block unauthorised gadgets from joining the network and transmitting information. They can house hundreds or even thousands of sensor nodes. Current wireless network routing systems allow for spoofing attacks, replaying routing information, and selective forwarding [5]. As a result, developing a trustworthy routing system for WSN is challenging. Physical attacks on the sensor nodes are simple to execute. By seizing sensor nodes, attackers can gain access to cryptographic keys and modify the code. Improving defences against node capture attacks is difficult work. When possible, the cluster head will send all discovered data to the next-level cluster head or the BS rather than keeping it in memory. The attackers may stop collecting data altogether. As a result, it is essential in WSN [7] to safeguard data aggregation.

Aggregated data is delivered to the BS in a standardised format after being collected from many sensor nodes. Either fresh information may be introduced into the network or the aggregation could fail if the compromised node was involved [8]. Existing solutions do not offer a cohesive response to the issue of data aggregation that is both energy-efficient and secure. Increased energy consumption at each sensor node due to complex security algorithms reduces the network's overall lifetime. When it comes to health monitoring systems, WSN shines brightest. The disclosure of private information can have serious repercussions, both professionally and personally. Most intrusion detection system (IDS) methods only search for network-layer threats and ignore other

Doi: https://doi.org/10.54216/JCIM.100205
Received: May 15, 2022 Accepted: August 18, 2022

layers, however an intrusion detection system in a WSN can uncover dangers that the prevention system missed [9].

2. Literature Review

The monitoring of a patient's condition while they are at home is the primary objective of the Alarm-Net system. The patient monitoring system integrates aspects of not one, not two, but all three levels of the internet. First-tier biosensors monitor vital signs such as heart rate, oxygen saturation, and electrocardiogram (ECG), in addition to tracking motion with accelerometers [10]. The information gathered in the first tier is transferred to the second tier, which is comprised of stationary sensors. The second tier of the home's security system is made up of sensors that monitor the environment in the home, including the air quality, temperature, lighting, and other factors. These fixed sensors provide the AlarmGate with the information that has been gathered by the biosensors. The sensors and the backend server are connected by AlarmGate, which acts as a bridge between the two [11]. This establishes a connection between the sensors and the IP network. The Alarm-Net approach is useful for managing power and safety in addition to its other applications.

With the use of an all-encompassing monitoring environment that includes implantable and wearable technology, doctors are able to keep a constant eye on patients' biological states and identify any irregularities that may pose a risk to their lives. The work station, the dominant attendant, the persistent record, the local processing unit (LPU), and the BSN node are the five components that make up the structural design of the system [12]. The biosensors that are located in the BSN node monitor an individual's vitals, such as their temperature, blood oxygen level, and heart rate, to evaluate their overall health. The data is sent from the BSN node to the LPU, which processes it and sends an immediate warning to the patient if anything out of the norm is discovered. Personal digital assistants (PDAs) and mobile phones both qualify as potential incarnations of the LPU. It fulfils the function of a router by establishing a connection between the BSN node and the primary server [13-14]. The database will keep real-time patient data as well as inquiries for an indefinite amount of time. It is possible for a mobile phone, laptop, or desktop computer to serve as the doctor's "work station" [15-16]. This allows the doctor to monitor the patient's vital signs and look for any anomalies that may be present. One of the shortcomings of the system is that it does not pay sufficient attention to the policies governing its security [17].

Patients will have access to a health monitoring system that is based on biosensors thanks to the programmable service architecture for mobile medical care. The information that was gathered is transferred to the wristwatch so that it can be examined [18-19]. The smartwatch acts as a client for the mobile care system, transmitting data over the HTTP POST protocol to the server. A current status report on the patient's health can be obtained by the physician by checking in with the mobile care server. However, the system does not have the appropriate safeguards in place, despite the fact that privacy and confidentiality are crucial for health data [20-22].

The lightweight verification algorithm that was suggested has it so that each node has multiple parents. Every child node is responsible for communicating its MAC address and message to the parent node. The parent node sends the fused message to the BS [23-25] while also include its own MAC set in the transmission. When a message is received, the BS will examine the message's MAC and compare it to the value that was previously fused in order to decide whether or not to accept the message. The BS is able to determine whether or not its customers are legitimate even if it does not receive individual authentication signals from each customer [26].

The method that the authors employed was one that aggregated encrypted data in WSN in a way that was both efficient and provably safe. A cryptosystem that is additively homomorphic is utilised by it in order to ensure the security of sensitive data. The sink node is given access to three variables: the header, which contains the IDs of all reporting nodes; the checksum, which ensures that the message has not been altered in transit; and the payload, which contains the data being sent to the sink node. In order to defend against the node exclusion attack, it is necessary for each node to generate a Message Authentication Code tag for its header [27]. The sink will only accept the header information if the result is in accordance with the tag. The strength of the method is based on the fact that the keys are created with the assistance of a completely untraceable pseudorandom generator. This method does have a few drawbacks, however, including the following: the Message Authentication Code is less effective at preventing internal attacks because it increases the computation complexity, requires the group key for the checksum, and a violation of the group key on any node threatens all of the other nodes in the network [28].

Continuous monitoring of a patient's physiological status as well as the detection of anomalies that could endanger the patient's life are both possible when a pervasive monitoring environment that supports wearable and implantable sensors is utilised. An LPU, a central server, a patient database, a work station, and a node for the Body Sensor Network (BSN) make up the five basic components that make up the architecture of the system. In order to assess an individual's state of health, biosensors, which may be found in the BSN node, monitor an

Doi: https://doi.org/10.54216/JCIM.100205
Received: May 15, 2022 Accepted: August 18, 2022

individual's vitals such as their temperature, blood oxygen level, and heart rate [29]. The data is transmitted from the BSN node to the LPU, which may be a cell phone or Personal Digital Assistant (PDA), and the LPU promptly notifies the patient if any anomalies are discovered in the data. It acts as a conduit for the transmission of data between the BSN node and the primary server. Current information as well as the results of searches performed in real time are stored in the database of patients. The vital signs of the patient are monitored on the physician's work station, which might be anything from a mobile phone to a desktop computer or even a laptop. The physician is on the lookout for any irregularities. One of the problems with the system is that it does not pay sufficient attention to the policies governing its security [30].

3. The Proposed Work:

The Blowfish algorithm makes better use of the resources it has at its disposal than the more traditional symmetric algorithms do. However, the computation time for security algorithms still needs to be reduced so that they can operate effectively in environments where there is more of a time constraint. At the same time, a reliable security system needs to be put into place. Therefore, investigations into lightweight cryptography techniques are being conducted. In order to determine which solution is superior, a number of symmetric and asymmetric algorithms that are efficient and compact are being developed. In contrast to their symmetric counterparts, asymmetric algorithms always make greater use of the data that is available. As a result of this, in this research study, we will analyse and compare the efficiency of lightweight symmetric algorithms in addition to other lightweight cryptographic approaches. By combining CP-ABE with the Speck method, which is the most lightweight symmetric technique available, confidentiality, veracity, and authenticity of medical data can be ensured.

An assortment of biosensors will be utilised in the future LSHS in order to monitor the patients' states of health. Using a method called lightweight SPECK, the sensitive health information has been encrypted. The encrypted medical records are sent to the repository for medical information. In addition to Speck, the CP-ABE access control method is implemented to ensure that only authorised physicians, nurses, and technicians are able to view patient information. Speck is used as the primary access control method.

3.1. Speck is a block and key size-flexible Add-Rotate-XOR cipher:

It works nicely with practically any computer system or microcontroller. It outperforms other lightweight algorithms in confined settings. Therefore, the current section of the study employs the Speck algorithm to encrypt sensitive medical information. Bitwise XOR, addition modulo, and left and right circular shifts are the building blocks of speck encryption. Below, we detail each phase of the encryption process.

i). The left word is rotated 8 bits to the left, and the right word is added to the resulting value.

ii). The left output is XORed with the round key and the result is the left input for the following round.

iii). The output is XORed with the output from the left side of the equation, and the right word is rotated three bits to the right. The result is used as the proper input in the subsequent iteration.

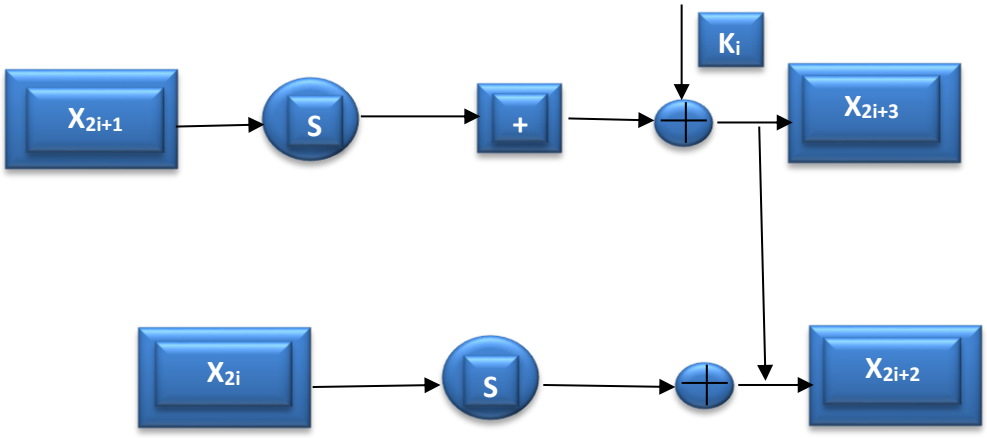

Figure 2: Round function of Speck encryption algorithm.

3.2. Cipher text-Policy Attribute Based Encryption (CP-ABE):

Doi: https://doi.org/10.54216/JCIM.100205
Received: May 15, 2022 Accepted: August 18, 2022

Access to patient information would be required for a large number of individuals, including the patient's loved ones as well as medical professionals and hospital employees. The diagnostic centre utilises cypher text-policy access control so that only authorised workers can view sensitive patient information. This keeps the information secure and protects the privacy of patients. The cypher text policy is used to encrypt the parameters of the public key, as well as an access structure and a message. The user's private key carries with it a one-of-a-kind collection of characteristics that together denote the user's access privileges. The communication has been encrypted, and only those users who possess the required traits will be able to decipher it. One of the attributes that is used in the process of generating a secret key in SHS is the patient id. The CP-ABE algorithm is comprised of a small number of phases.

i). Secret key and authentication key is created.

ii). The message M, the entrée arrangement 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.

Initially, we premeditated a node (UAV) - important milieu $NK = \left[NK_{i,k}\right]_{N\times K}$, which provides the relation amongst nodes and solutions (eq. (1)).

$$NK_{i,k} = \begin{cases} 1 & if\ K_k \in N_i \\ 0 & Otherwise \end{cases} \tag{1}$$

Afterward that a key-pathway matrix $KP = \left[KP_{k,j}\right]_{K\times P}$ is assessed, which offers the connection amongst the keys and pathways (eq. (2)).

$$KP_{k,j} = \begin{cases} 1 & if\ K_k\ can\ use\ by\ P_j \\ 0 & Otherwise \end{cases} \tag{2}$$

Where P is the numeral of pathways, K is the numeral of solutions, K_k is the k^{th} key in the key`s cluster and P_j is the j^{th} path of FANET.

A node-path milieu $NP = \left[NP_{i,j}\right]_{N\times P}$ is attained by proliferating the matrix NK and KP, which produces the connection amongst nodes and pathways (eq. (3)).

$$NP = NK \times KP \tag{3}$$

If a association amongst nodes is protected by extra than one strategic or nodes convey more than one data package, then additional connection amongst nodes and pathways is estimated as $NPL = \left[NPL_{i,j}\right]_{N\times P}$. (eq. (4))

$$NPL_{i,j} = \frac{1}{l}\sum_{a=1}^{l} \frac{\left|K_i \cap K_{a,a+1}\right|}{\left|K_{a,a+1}\right|} \tag{4}$$

Where l signifies distance of a association, $K_{a,a+1}$ signifies distribution solutions of a^{th} link.

Afterward that we association the two mediums NP and NPL to a single medium $NPM = \left[NPM_{i,j}\right]_{N\times P}$. (eq. (5))

$$NPM = \delta \times NP + (\delta - 1) \times NPL \tag{5}$$

Doi: https://doi.org/10.54216/JCIM.100205
Received: May 15, 2022 Accepted: August 18, 2022

Where δ is a continual whose cost designated from (0, 1).

At latest with the assistance of NPM, we attain a node`s contribution medium $NPM_i = \lfloor NPM_{i,j} \rfloor_{N\times 1}$. (eq. (6))

$$NPM_i = \begin{cases} \sum_{j=1}^{P} NPM_{i,j} & participation\ of\ node\ N_i \\ 0 & Otherwise \end{cases} \quad (6)$$

Initially planned process is employed for grouping (clustering) the nodes by examining the inconsistency. It is detached the altogether nodes into K groups by eq. (7).

$$E_D = \sum_{\phi=1}^{K} \sum_{\rho=1}^{N_u} E_d{}^2 (C_\phi - X_\rho) \quad (7)$$

Here $E_d{}^2 (C_\phi - X_\rho)$ specifies a square of Euclidean detachment from ϕ^{th} centroid to ρ^{th} node of group and N_u displays numeral of nodes.

Data collected by biosensors and transmitted to a medical repository are encrypted using the Speck algorithm in LSHS. Only licensed medical personnel are permitted access to the health records maintained in the medical repository. In order to regulate entry to the LSHS, CP-ABE has been installed. Collusion assaults cannot compromise CP-ABE. It ensures the privacy of user information, user authentication, and restricted access. The LSHS is safe from timing and collusion attacks as well, thanks to the incorporation of the Speck and CP-ABE algorithms.

4. Result and Discussion:

All methods that use symmetric keys can guarantee the user's privacy and security, but they cannot guarantee the user's authenticity. In order to ensure that the findings of this study are credible, the Speck algorithm and the CP-ABE were combined. When comparing the efficacy of Speck and CP-ABE to that of Blowfish and CP-ABE, the former has been found to be more effective. Both Table 1 and Table 2 present a comparison between Blowfish and CP-ABE and Speck and CP-ABE in terms of the amount of time required for encryption (ET), the amount of time required for decryption (DT), the amount of time required for overall computation (CT), and the amount of energy consumed (EC). When compared to Blowfish and CP-ABE on their own, the encryption and decryption times produced by the combination of Speck and CP-ABE are significantly faster, and the overall computing time is reduced.

The following equation is utilised in the process of calculating energy consumption. The production of keys, encryption, and decryption are all processes that consume energy, which contributes to the overall amount of energy that is used. The energy requirements of Speck and ABE are significantly lower than those of Blowfish and ABE. Authentication, authorization, and access management can be accomplished with increased speed and accuracy thanks to the collaborative efforts of Speck and ABE, which also protect newly created data from potential threats.

$$Energy\ Consumption\ (EC) = Vx\ I\ x\ \Delta T \quad (1)$$

Table 1: The performance comparison of the proposed method with existing approach.

Methods	File Size									
	50		200		400		1500		3000	
	ET	DT	ET	DT	ET	DT	ET	DT	ET	DT
Blowfish and CP-ABE (s)	0.9	2.48	0.93	3.67	2.46	4.29	7.8	5.69	8.78	6.67
Proposed	0.56	2.12	0.88	2.53	1.42	3.11	5.91	4.35	7.38	5.37

Doi: https://doi.org/10.54216/JCIM.100205
Received: May 15, 2022 Accepted: August 18, 2022

Method (s)										

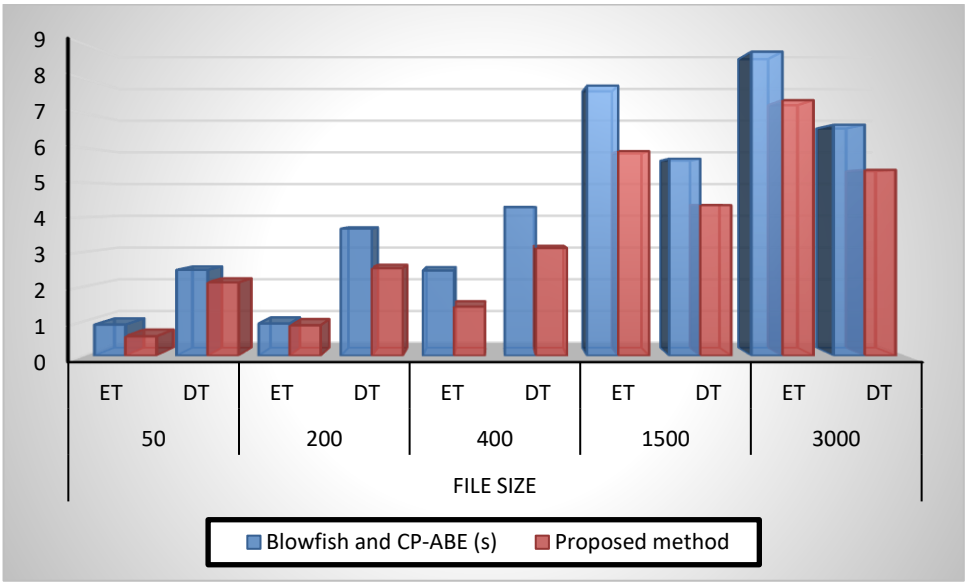

Figure 3: The performance comparison of the proposed method with existing approach.

It can be concluded from Table 1 and Figure 3 that the proposed algorithm encryption time and decryption time is lesser than the cascaded approach of Blowfish and CP-ABE (s). Which proves the success of the proposed algorithm.

Table 2: The performance comparison of the proposed method with existing approach.

Methods	File Size									
	50		200		400		1500		3000	
	CT	EC	CT	EC	CT	EC	CT	EC	CT	EC
Blowfish and CP-ABE (s)	5.4	0.023	7.5	0.023	8.6	0.052	12.4	0.187	15.1	0.175
Proposed Method (s)	3.6	0.013	6.7	0.019	7.4	0.031	10.2	0.122	14.3	0.186s

Doi: https://doi.org/10.54216/JCIM.100205
Received: May 15, 2022 Accepted: August 18, 2022

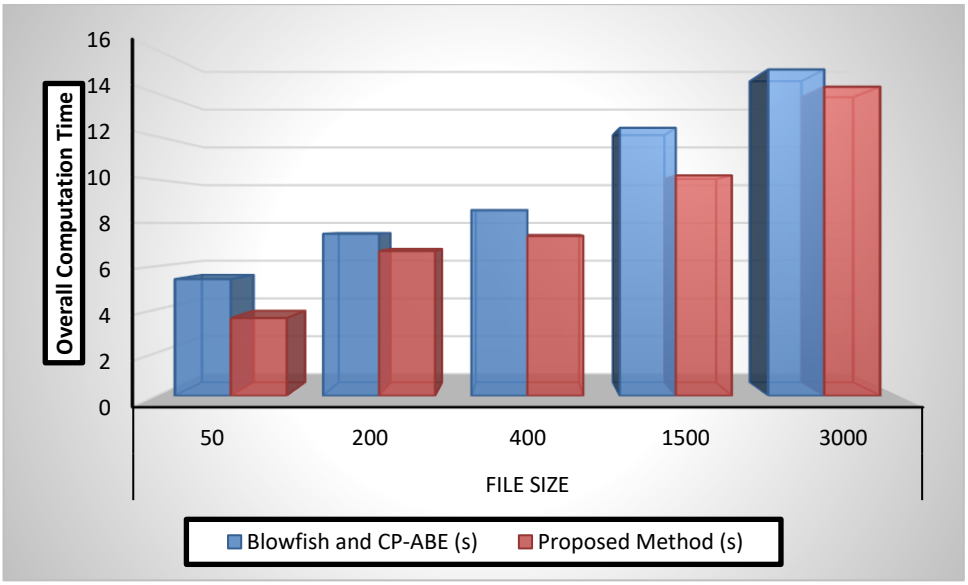

Figure 4: The Overall computation time comparison of the proposed method with existing approach.

Memory, processing time, and key size are three areas where lightweight algorithms excel in comparison to their more resource-intensive counterparts. Low-overhead cryptographic methods sacrifice security for efficiency. Security, efficiency, and low resource usage are all improved for medical software.

Cryptographic approaches that use less power are necessary for devices that run on batteries. Lightweight cryptographic algorithms can be used by sensors that rely on less power, such as medical sensors, environmental sensors, and so on. Low latency and instantaneous responsiveness are also necessary for some applications. Lightweight cryptographic approaches may be used, for instance, by the sensor node that is active during transmission but inactive otherwise. The immediate-response automotive electronics can likewise benefit from lightweight cryptography approaches. Research into WMSN's security is particularly important because of the prevalence of low-power devices used in healthcare applications. When compared to more complex cryptographic algorithms, lightweight cryptographic methods are ultimately deemed superior.

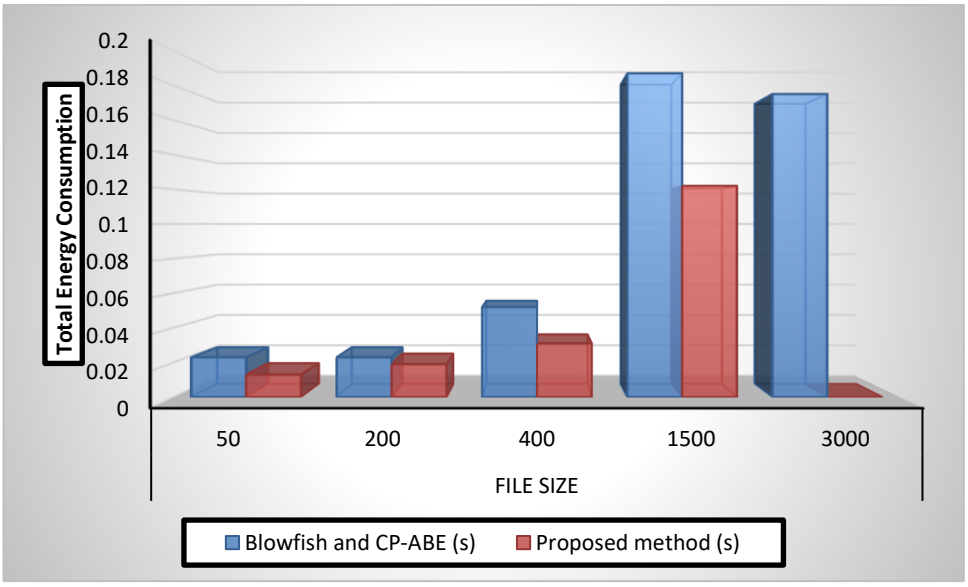

Figure 4: Total Energy consumption comparison of the proposed method with existing approach.

Doi: https://doi.org/10.54216/JCIM.100205
Received: May 15, 2022 Accepted: August 18, 2022

Form Table 2 and Figure 3 and 4, conclusion can be drawn that the proposed algorithm outperforms than the existing algorithm. Even such asymmetric algorithms protect users' privacy, data, and identity, their complex nature stems from their large key sizes. Since both parties share the same key, authentication and non-repudiation are not possible with a symmetric technique. Therefore, the CP-ABE has been integrated into the proposed system to ensure security. Both the security features and the resource limitations of the sensor network can be met by combining the Speck and CP-ABE algorithms. These cryptographic algorithms are a type of IDS that does not safeguard a network from every possible assault.

5. Conclusion:

Any changes that the sensor nodes of a WSN detect in the physical world that surrounds them are communicated back to the BS by the network. Sensor networks combine the information that they collect in order to reduce costs associated with connectivity, the amount of power that is consumed, and redundant data. Protecting this information is a pressing area of research that needs to be done as soon as possible because of how easily adversaries can get sensor data. There have been many developments in security procedures, but there hasn't been much of an impact on the amount of electricity they consume. WSN has recently been used to a number of other uses. Data security and energy consumption are two important research areas in wireless sensor networks (WSN). The fundamental objective of this research is to devise a cutting-edge algorithm that can ensure data safety while consuming a minimum amount of available resources. This study recommends using LSHS as a method for securing health data while causing the least amount of effect possible. Before the data is sent to the medical repository, it is encrypted using the Speck lightweight symmetric approach. This technique was developed by Microsoft. CP-ABE is in charge of maintaining the confidentiality of all of the medical records. Due to the lack of authenticity given by symmetric algorithms, CP-ABE incorporates both the Blowfish and Speck methods. Both Speck and CP-ABE provide performance that is superior to that of existing alternatives.

Funding: "This research received no external funding"

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

References

[1]. Beaulieu, R, Shors, D, Smith, J, Treatman-Clark, S, Weeks, B & Wingers, L 2015, "Simon and Speck: Block Ciphers for the Internet of Things", Cryptology ePrint Archive Report, pp. 1-15.

[2]. Boubiche, DE & Bilami, A 2012, "Cross Layer Intrusion Detection System for Wireless Sensor Network", International Journal of Network Security and its Applications, vol. 4, no. 2, pp. 35-52.

[3]. Brindha, K & Sudha, S 2015, "Analysis of Homomorphic Cryptosystems", Asian Research Publishing Network Journal of Engineering and Applied Sciences, vol. 10, no. 12, pp. 5206-5212.

[4]. Butun, I, Morgera, SD & Sankar, R, 2014, "A Survey of Intrusion Detection Systems in Wireless Sensor Networks", IEEE Communications Surveys and Tutorials, vol. 16, no. 1, pp. 266-282.

[5]. He, D, Chan, S & Tang, S 2014, "A Novel and Lightweight System to Secure Wireless Medical Sensor Networks", IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 1, pp. 23-32.

[6]. 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.

[7]. 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.

[8]. McKay, KA, Bassham, LE, Turan, MS & Mouha, NW 2017, "Report on Lightweight Cryptography", National Institute of Standards and Technology, pp. 1-27.

[9]. 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.

[10]. Xu, S & Wang, J 2016, "A fast incremental extreme learning machine algorithm for data streams classification", Expert Systems with Applications, vol. 65, pp. 332- 344.

Doi: https://doi.org/10.54216/JCIM.100205
Received: May 15, 2022 Accepted: August 18, 2022

[11]. Xun, Y, Athman, B, Dimitrios, G, Andy, S & Jan, W 2015, "Privacy Protection for Medical Sensor Data", IEEE Transaction on Dependable and Secure Computing, vol. 13, no. 3, pp. 369–380.

[12]. H. Wang, Y. Yuan, and X. Wang, "Cybersecurity in the Internet of Things: Emerging Threats and Countermeasures," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8076-8091, Oct. 2019, doi: 10.1109/ JIOT.2019.2925034.

[13]. W. Serwe, "Formal specification and verification of fully asynchronous implementations of the data encryption standard," Computer Science, vol. 196, pp. 61–147, 2015.

[14] L. Lu, Zhongguo yi liao qi xie za zhi; Chinese journal of medical instrumentation, vol. 42, no. 3, pp. 180-181, 2018.

[15] C. Han, X. Yang, and W. Hu, "Chaotic reconfigurable ZCMT precoder for OFDM data encryption and PAPR reduction," Optics Communications, vol. 405, no. 2, pp. 12–16, 2017.

[16]. C. Wei, "Application of data encryption technology in computer network security," Journal of Physics: Conference Series, vol. 1237, no. 23, Article ID 022049, 2019.

[17] 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.

[18] 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.

[19] 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.

[20]. 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.

[21]. M. Wahid, A. Ali, B. Esparham, M. Marwan. "A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention". J. comput. sci. inf. tech.2018; vol. 3, no. 2, pp. 218–230.

[22]. S. Pavithra, E. Ramadevi. "Performance Evaluation of Symmetric Algorithms". J. glob. res. comput. sci. technol.2012; vol. 3, pp. 44–45.

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

[24]. D. Benhaddou, A. Al-Fuqaha. "Wireless Sensor and Mobile Ad-Hoc Networks: Vehicular and Space Applications". New York, NY.: Springer New York, 2015.

[25]. O. Olakanmi, A. Dada. "Wireless Sensor Networks (WSNs): Security and Privacy Issues and Solutions". In Wireless Mesh Networks - Security, Architectures and Protocols, London, UK. Intech Open Limited, 2020.

[26]. D. Kandris, C. Nakas, D. Vomvas, G. Koulouras. "Applications of Wireless Sensor Networks: An Up-toDate Survey", Appl. Syst. Innov.2020, vol. 3, no. 1, p. 14.doi:10.3390/asi3010014

[27] C. Lee. "Security and Privacy in Wireless Sensor Networks: Advances and Challenges". Sensors, 2020; vol. 20, no. 3, p. 744. https://doi.org/10.3390/s20030744.

[28]. M. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini and Y. Khamayseh, "Comprehensive study of symmetric key and asymmetric key encryption algorithms", 2017 International Conference on Engineering and Technology (ICET), 2017. Available: 10.1109/icengtechnol.2017.8308215

[29]. Z. He, L. Wu and X. Zhang, "High-speed Pipeline Design for HMAC of SHA-256 with Masking Scheme", 2018 12th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID), 2018. Available: 10.1109/icasid.2018.8693229.

[30]. S. Srinivasan, K. ShivaKumar and M. Muazzam, "HMAC-RSA: A security mechanism in cognitive radio for enhancing the security in a radio cognitive system", Journal of Intelligent & Fuzzy Systems, vol. 36, no. 5, pp. 4449-4459, 2019. Available: 10.3233/jifs-169999.

Doi: https://doi.org/10.54216/JCIM.100205
Received: May 15, 2022 Accepted: August 18, 2022