Secure Transmission of Healthcare Data in Heterogeneous Networks

Jansi Rani Amalraj[1], Robert Lourdusamy[2]

[1]Assistant Professor, Department of Information Technology, Nirmala College for Women,
Coimbatore -641 018, India,
[2]Associate Professor, Department of Computer Science, Government Arts College,
Coimbatore -641 018, India,

Abstract

Securing patient health records within heterogeneous networks is imperative to ensure data security, privacy, integrity, and confidentiality at all times. The vulnerability of critical data within heterogeneous networks underscores the potential consequences of unauthorized access, ranging from job loss to mental distress for the patient. The exchange of medical data within heterogeneous network architecture is a critical component of modern healthcare systems, enabling seamless sharing and access to patient information across diverse platforms and healthcare providers. An enhancement to existing security techniques is required in the Heterogeneous Network within a healthcare environment. To mitigate this risk, this paper introduces the Secure Secret Key Sharing based Strong Cryptography (S4C) algorithm. The encryption and decryption time during transmission is evaluated both in Electronic Code Book (ECB) mode and CBC (Cipher Block Chaining) mode, aiming to securely exchange medical data between networks and to enhance overall data security.

Keywords: Security, ECB mode, CBC mode, encryption, decryption

1. Introduction

Medical sensors play a crucial role in monitoring a patient's health and transmitting vital data to healthcare providers or hospital servers. However, the transmission of this sensitive information can be susceptible to security threats. For example, malicious individuals may intercept the data as it travels over wireless channels and manipulate the results [1]. Subsequently, they could transmit the altered data to healthcare professionals or the server, posing a significant risk to patient safety. Considering the vulnerability of patient privacy, ensuring robust security measures becomes imperative when integrating technology into healthcare environments. The storage, usage, and handling of a patient's vital information should be approached with the utmost care, and this is particularly crucial for individuals with health conditions that society may consider as socially unacceptable. Mishandling such sensitive health information can have far-reaching consequences, including humiliation, inappropriate treatments, strained relationships, and even the risk of losing one's job [1]. Moreover, health data that is perceived unfavorably may impede a person's access to health insurance coverage. Consequently, it is imperative to prioritize the secure and confidential storage and transmission of this data to protect the privacy and well-being of the individuals involved.

In healthcare, the need for interoperability and efficient data exchange is a paramount to enhance patient care, diagnosis, treatment, and overall healthcare outcomes. Heterogeneous network architectures facilitate the integration of various medical devices, Electronic Health Records (EHR) systems, wearable technologies, mobile apps, and other healthcare applications into cohesive network. This integration optimizes the utilization of available healthcare data and promotes a comprehensive view of a patient's medical history and ongoing treatment. To cater to the unique needs of end-users, these sensors are purposefully designed. As an illustration, an EEG sensor is customized for brain-electrical activity monitoring, while an ECG sensor is specifically designed for monitoring heart behaviors.

The nodes can be divided into the following classifications based on their implementation:

- **Implant Node:** Nodes that are implanted can be located beneath the skin or within the human body.
- **External Node:** This kind of node does not establish direct communication with the individual's body and is typically positioned at a short distance, ranging from centimeters to 5 meters, away from the person's physique.
- **Body Surface Node:** This node can be either attached to the body's surface or situated at a distance of approximately 2 centimeters from the human body.

A robust security mechanism with an efficient key generation process, capable of meeting critical data security is evaluated in Electronic Code Book (ECB) mode and CBC (Cipher Block Chaining) mode. The rest of this paper is organized as follows. Section II introduces the background of Wireless Body Area Networks (WBAN) framework. Section III provides the associated literature reviews of the medical data exchange between networks. Section IV presents the communication architecture of heterogeneous network. Section V examines proposed method with the traditional approaches. Finally, Section VI brings the papers overarching theme to a close.

2. WBAN framework

Within the framework of WBANs, based on three types of nodes are defined based on their network specific functions:

- ○ **Coordinator:** Functions as an intermediary establishing connections with the external environment, other WBANs, or serving as a trust center. Typically, a PDA assumes the role of the WBAN coordinator, facilitating communication with all other nodes.
- ○ **End Nodes:** The node primarily concentrates on executing its embedded applications; however, it does not possess the capacity to broadcast data to other nodes within the network.
- ○ **Relay:** Acts as intermediaries within the network that consist of both parent and child nodes. These nodes play a crucial role in relaying messages and gathering data from other nodes. In cases where a node falls out of the transmission range, relay nodes facilitate the transfer of information to the PDA by passing it through the network.

Data security typically revolves around three fundamental characteristics:

- **Integrity:** preventing unauthorized modification of the data
- **Confidentiality**: preventing unauthorized disclosure of the data
- **Availability:** Preventing the wrongful retention of data without authorization.

2. Related works

This section covers the key aspects for medical data exchange between networks to transfer medical data in a secured manner that gains a clearer insight into the research problems.

Pushpa et al. [2] presented a novel hybrid information encoding framework for safeguarding diagnostic information within medical imagery. Utilizing various performance measures ensures, that the proposed technique’s outcomes are tested against different benchmark images, yielding positive results. This model integrates the 2D discrete wavelet transform with a hybrid encryption scheme. The utilization of WBANs has extended among distant healthcare and various domains such as military, sports, disaster relief and more. As the network scale grows, the number of nodes increases, and the links become more complex. This development, have made energy-saving conservation and data security become more prominent issues. In the paper by Peng et al. [3], authors propose a chaotic compressive sensing (CCS) for addressing the above mentioned critical challenges concurrently. In contrast to the typical compressive sensing method, CCS is utilized to conserve a considerable volume of storage capacity, solely demanding the storage of the matrix creation parameter. Furthermore, Chaos sensitivity enhances data transmission security. A modified CCS for image transmission includes confusion and masking encryption, significantly improving security. Simulations confirmed the effectiveness and feasibility of these enhancements Gupta et al. [4] proposed a chaos-based encryption scheme designed to enhance the security of medical images. The primary idea involves encrypting and decrypting images by employing a combined sequence of keys generated from the Logistic map and Duffing map to shuffle neighboring pixels. A consolidate key sequence referred to as {Ka}, is created using the key sequences from both maps combined through XOR, which is then used for image encryption. The proposed scheme's security is evaluated through visual analysis, histogram examination, and correlation coefficient analysis, ensuring robust data protection. Huang et al. [5] introduced a healthcare system (HES) developed to collect clinical information from WBANs, transmit this through an extensive wireless sensor network infrastructure, and subsequently, publish it into wireless personal-area networks through a gateway. Moreover, HES employs a send-receive model scheme to achieve key distribution and secure data transmission, utilizes homomorphic encryption based on a matrix scheme to ensure privacy, and included an expert system capable of analyzing the encrypted medical data and providing automated feedback on the results. Abid et al. [6] explored the influence of Blockchain on the health care industry, with a specific focus on improving enhancing secure information sharing between medical record repositories and healthcare institutions for research purposes. The authors proposed blockchain architecture for managing patient data. And also discussed the characteristics of blockchain from a healthcare standpoint and recommended a transformation in medical record management. Pirbhulal et al. [7] constructed a security framework that ensures decentralized and protected communication while taking into account the mentioned aspects for IoMT-oriented healthcare applications. Considering the individual's distinct physical and biological characteristics, bodily attributes can be employed to enhance IoMT security. Consequently, bio-keys are produced in the suggested security framework to heighten the challenge for unauthorized access to medical data. Experimental findings demonstrate that the devised model surpasses current methods in the realms of random key generation and energy consumption. Vijayalakshmi et al. [8] proposed hybrid security techniques to secure healthcare information. The security method relies on data masking and encryption mechanisms to thwart access by intruders and unauthorized individuals. Consequently, this strategy capitalizes on the secure transfer of medical information. Fadheel et al. [9] introduces an HIE (Health Information Exchange) system that focuses on enhancing the privacy and security of patient data shared among healthcare providers. PHeDHA is based on the ADB-TTP scheme. ADB-TTP combines Active Data Bundles (ADBs) with the involvement of a trusted third party (TTP) to safeguard patient healthcare data, especially sensitive information. ADBs are software objects that not only protect healthcare data but also include metadata that defines the data and sets access and privacy policies. These policies are enforced by a policy enforcement engine, often referred to as a virtual machine (VM), within the ADB. The VM ensures data integrity and compliance with the metadata-defined policies. Elhoseny et al. [10] suggested a blended security framework designed to protect diagnostic textual information within medical visuals. This framework combines 2D-DWT with steganography and a hybrid encryption scheme, featuring the Advanced Encryption Standard and RSA algorithms. The process involves encrypting sensitive data and then hiding the encrypted data within a cover visual, utilizing either 2D-DWT-1L or 2D-DWT-2L. The assessment of this framework employs six statistical criteria: PSNR, MSE, BER, SSIM, SC, and correlation. In color visuals, PSNR varies from 50.59 to 57.44, whereas in black-and-white images, it extends from 50.52 to 56.09. MSE metrics fluctuate between 0.12 to 0.57 for color visuals and 0.14 to 0.57 for grayscale representations. Both categories display no BER, and SSIM, SC, and correlation values highlight substantial resemblance between hidden and initial data in both color and grayscale visuals. Shaikh et al. [11] proposed the design and development of a security-enhanced ECG (Electrocardiogram) system aimed at safe and privacy-preserving ECG visualization and diagnosis. The system primarily uses the QRS complex technique for diagnosing ECG signals and assessing a patient's health status. It can detect critical conditions and trigger alerts for further diagnosis, aiding both medical practitioners in arrhythmia detection and medical researchers in their studies. The system places a strong emphasis on privacy and security by implementing techniques to safeguard the genuineness and confidentiality of patient healthcare information. This is achieved through signal encryption, which ensures that sensitive medical information remains confidential and secure during data transmission and processing. Liu et al. [12] presents an algorithm designed for large medical datasets. It leverages 3dimensinonal hyperchaos and a 3 dimensional dual-tree complex wavelet transform, combining visual perception characteristics with perceptual hashing. Algorithm scrambles the watermark for security, utilizes low-frequency factors from a 3D DTCWT-DCT transformation for key generation, and employs zero embedding and blind extraction to protect the initial healthcare information. It proves effective against common and geometric attacks, preserves critical features, conserves bandwidth, and ensures the safe exchange and safekeeping of large medical datasets in the Internet of Medical Things. Giri et al. [13] introduced a new security protocol called SecHealth, designed for situations where information is transmitted by healthcare sensors transmit to a nearby fog server. This procedure guarantees that data exchange can exclusively happen following mutual authentication between the sensor and the fog server. Security analysis of SecHealth demonstrates its effectiveness in thwarting all known possible attacks, making it a robust solution for securing healthcare sensor data transmission to fog servers. Hussein et al. [14] introduces a system to secure medical image storage and sharing is proposed, leveraging cryptography techniques like ECC, AES, and SHA-3. To reduce client-side computational overhead, a third-party auditor verifies image integrity before cloud storage. Digital signatures ensure data source authentication and robustness against unauthorized access or modification attempts. The system is highly secure, offering ample storage capacity with reasonable computational and storage overhead. It enhances medical data security during transmission and storage on the cloud. Advances in medical devices and communication technologies enable the transfer of medical data via wireless body sensor networks. However, a major challenge in smart healthcare is the sensitivity of patient information, emphasizing the critical need for secure data transmission. Pirbhulal et al. [15] discussed the topic of secure and safe communications within the context of smart and connected healthcare. Rajagopalan et al.

[16] discusses secure communication in smart healthcare, focusing on a server-client model proposed. The process involves encrypting medical images using AES and enhancing security with an embedded One Time Password (OTP) generated via the Tent map. The OTP-embedded picture is distributed over an intranet. Authorized users receive the OTP via GSM, compare it with the one extracted from the image, perform integrity checks, and decrypt the medical record. The encryption method is implemented in Python 2.7 and validated through various tests, including entropy, correlation, differential, error metrics, and NIST assessments, ensuring robust and secure medical image communication. Srivastava et al. [17] introduced a security framework for mHealth applications, offering features like authentication, authorization, secure data storage, and transmission. This framework is adaptable to both new and existing mHealth apps and effectively addresses security and privacy concerns. The authors demonstrated its utility by creating a sample mHealth app based on this framework, showing that it seamlessly enhances security and privacy without compromising the user experience. In essence, the framework provides a practical solution to safeguard medical data and workflows in the mHealth environment, ensuring both the integrity of health information and user trust. Ara et al. [18] have put forward a secure privacy-preserving data aggregation (SPPDA) scheme is introduced for remote health monitoring systems, focusing on enhancing data aggregation efficiency and privacy. This scheme leverages bilinear pairing and combines homomorphic properties of the bilinear ElGamal cryptosystem with aggregate signatures for data authenticity and integrity in Wireless Body Area Networks (WBANs). The SPPDA scheme ensures data confidentiality, authenticity, and privacy while resisting passive eavesdropping and replay attacks. It offers semantic security based on the decisional bilinear Diffie-Hellman assumption.

Tutari et al. [19] proposed a continuous role-based authentication technique for monitoring users and Implantable Medical Devices (IMDs) during computer interactions. This addresses security concerns with wireless connectivity that could potentially compromise IMD data, risking patient safety. The protocol offers secure data transmission for computer-IMD interactions, considering the limited resources of IMDs, including memory and battery power. It ensures continuous protection while minimizing the impact on the IMD's functionality. Hashim et al. [20] proposed a novel steganography scheme called BIS, using three random control variables selected through Henon Map Function (HMF). This scheme combines Affine cipher and the Huffman method for encoding and data reduction before embedding, increasing payload capacity. The integration is effective for checking and mapping bits (0 and 1) while incorporating and partitioning concealed information to map every bit in the stego image. Findings show that the scheme safeguards medical data secrecy and safety while preserving image quality. Braham et al. [21] have conducted comprehensive review of Body Area Network (BAN) communication standards, security threats, and vulnerabilities. Based on this review, it proposes reference security architecture, with a primary focus on the BAN layer (Tier 1). This architecture integrates the Wireless Body Area Network (WBAN) standard (IEEE 802.15.6) to establish a robust security foundation. The goal is to support BAN manufacturers and auditors in developing and ensuring secure BAN systems, addressing critical security and privacy concerns in BAN-based healthcare applications.Vezeteu et al. [22] introduced an efficient and secure transmission framework for personal data obtained through optical character recognition (OCR). Challenges in patient information processing in the medical care framework are addressed, utilizing this system. This process involves capturing the information from an ID document, encrypting it, sending it to the cloud, decrypting it, and then using OCR software for data extraction. Additionally, the system allows medical personnel to communicate and share patient information through a chat server, enabling consultations and second opinions. This approach significantly reduces data entry time and fosters collaboration among medical specialists, enhancing patient care and data security. Qiu et al. [23] introduced secure data storage and distribution technique that uses selective encoding, fragmentation, and dispersion to safeguard data privacy, even in cases of compromised transmission media and encryption keys. This user-centric approach places data protection in the hands of the end user, typically on a trusted device like a smartphone. The technique empowers end users to manage access and sharing of their information. The authors present a demonstration of the technique's efficiency through a performance evaluation on a smartphone platform, emphasizing its effectiveness in enhancing data security and privacy. Chi et al. [24] introduced e-SAFE, an innovative scheme enhancing security and safety for Implantable Medical Devices (IMD). It incorporates an efficient encryption approach driven by compressive sensing, simultaneously encoding and compressing IMD information, resulting in a reduction of over 50% in information exchange overhead while preserving data usability and confidentiality. Additionally, e-SAFE offers protocols for device pairing, dual-factor authentication, and accountability-enabled access. Security analysis and performance evaluation affirm the scheme's validity and efficiency, making it a valuable advancement in safeguarding IMDs and their data. Amofa et al. [25] presented a blockchain-supported system for safe management of individual health data for exchanging information. This user-centric system pairs user-generated acceptable usage policies with smart contracts to minimize data risks and enable post-sharing data control. Health service providers benefit from increased data management assurance. Experimental results support the efficacy of this approach, offering a promising solution for secure and user-controlled health data sharing, with room for further developments. Vidya et al. [26] proposed an invisible watermarking technique for embedding Electronic Patient Records (EPR) into facial images, secured by a novel Restoration & Bundle Encryption method. This method utilizes the patient's bioelectric signal for key generation, ensuring data protection. Security evaluation confirms the inability to extract information without the key within a reasonable timeframe. Simulation results demonstrate superior performance, with a high PSNR, 93% NC, minimal contrast variation, and low correlation difference. High entropy and low variance highlight minimal medical information loss during the de-watermarking process, underscoring the method's effectiveness.

3. Communication architecture of Heterogeneous network

First, the communication architecture in each of these networks should be understood, to determine the appropriate security mechanism to implement in a diverse network environment. This involves acquiring insights into communication, both externally and internally, while taking into account interactions with the external environment and concurrently existing heterogeneous networks.

Consequently, a concise summary of the communication architecture within heterogeneous networks is discussed. Figure 1 illustrates the architecture for medical data exchange between heterogeneous networks.

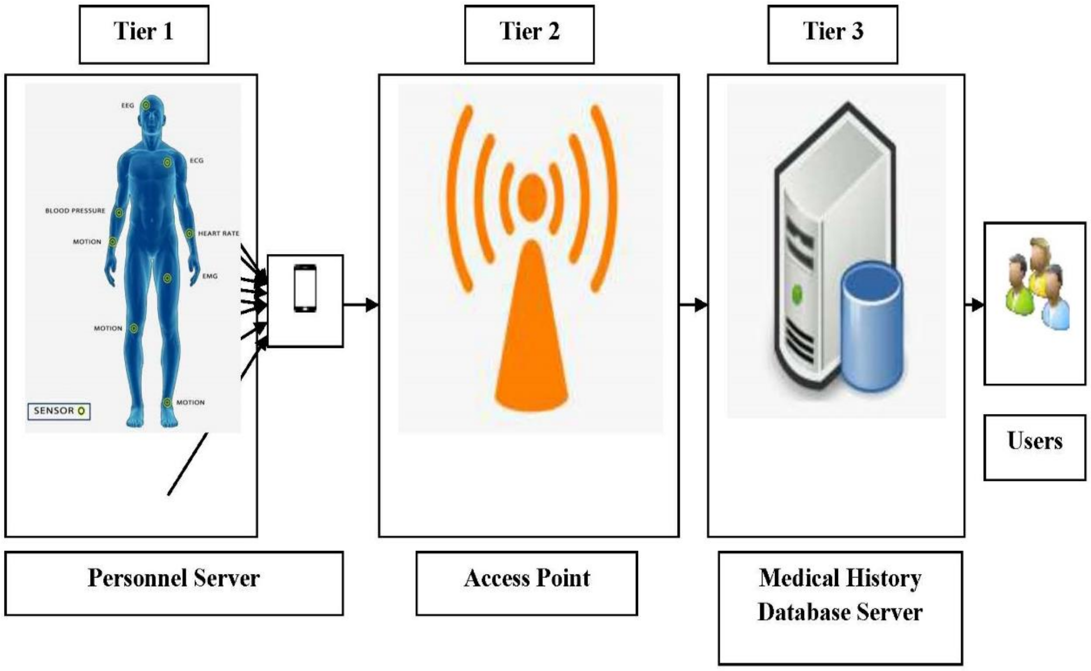


Figure 1: Medical data exchange between heterogeneous network architecture

4. Proposed Work

In existing systems, AES, DES, RSA ECC, and other cryptography algorithms [24] are used to exchange medical data securely between networks. While using these algorithms, it is crucial to keep the encryption and decryption keys highly secret, as their disclosure could have severe consequences. However, the challenge lies in the delicate balance between maintaining key confidentiality and ensuring availability. Conventional encryption methods struggle to achieve both reliability and confidentiality simultaneously. The dilemma arises when storing the encryption key: choosing between a single highly confidential key copy and multiple copies distributed across different locations for enhanced reliability. Augmenting key reliability through multiple copies compromises secrecy by creating additional attack vectors, increasing the risk of a copy falling into the wrong hands. The critical contributions of the Secure Secret key Sharing based Strong Cryptography algorithm(S4C) addresses the above issue.

The steps involved are as follows:

- The S4C algorithm is employed for the secure distribution of a confidential code, frequently utilized for safeguarding additional encryption keys.
- The confidential information is fragmented into several segments, referred to as "shares," which serve the purpose of reassembling the initial secret.
- In order to unlock the secret with the S4C algorithm, the user needs to possess the minimum number of shares, referred to as the "threshold." This threshold signifies the lowest number of shares essential to access the secret.
- This technique can be employed to encrypt the vault's access code and create a designated number of shares (denoted as "Ns").
- The access to the vault is only possible through the collective effort of combining these shares. The threshold may be customized according to the count of executives, guaranteeing that authorized

personnel maintain constant access. Even if one or two shares end up in unauthorized possession, accessing the access code would remain unattainable unless cooperation from the other executives is secured.

4.1 Block Diagram of S4C Algorithm

To transmit a packet to the Medical History Database Server (MHDS), the Personnel Server (PS) initiates the process by generating cryptographic keys. The Keys generated using are assigned as public key (for encryption) and secret key (for decryption). Therefore, to achieve proper decryption, it is vital to ensure a secure sharing of the secret with the user. Hence, the Personnel Server creates secret key. Subsequently, it sends each share to the user via both the Access Point (AP) and the MHDS. Once the user has received each share, they can reconstruct the secret key. After the secret sharing is complete, the Personnel Server obtains Sensor Readings (SR) from the human body and encrypts these readings using the public key. Then it transmits ciphertext to MHDS via AP. Figure 2 illustrtes the block diagram of S4C algorithm.

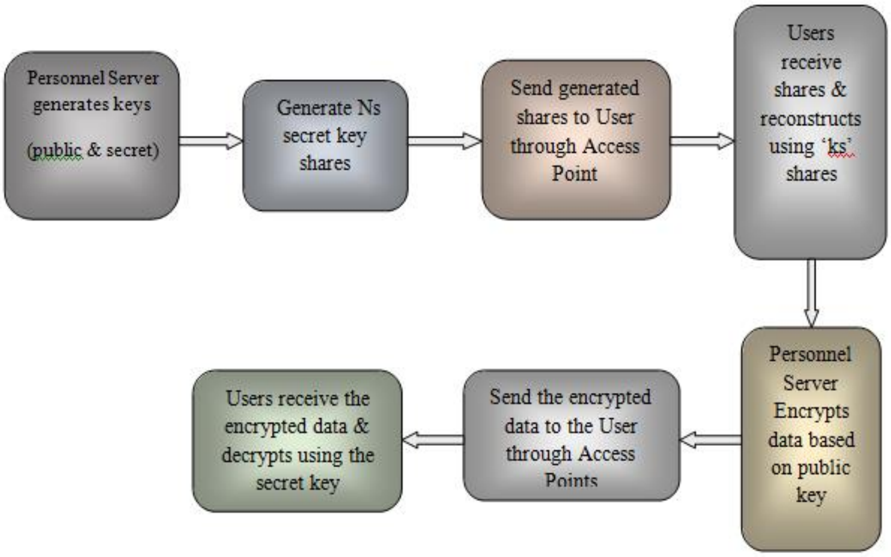

Personnel Server generates keys (public & secret)
Generate Ns secret key shares
Send generated shares to User through Access Point
Users receive shares & reconstructs using 'ks' shares
Personnel Server Encrypts data based on public key
Send the encrypted data to the User through Access Points
Users receive the encrypted data & decrypts using the secret key

Figure 2: Block Diagram of S4C Algorithm

The steps involved at the Personal server side and the user side is illustrated in Figure 3.

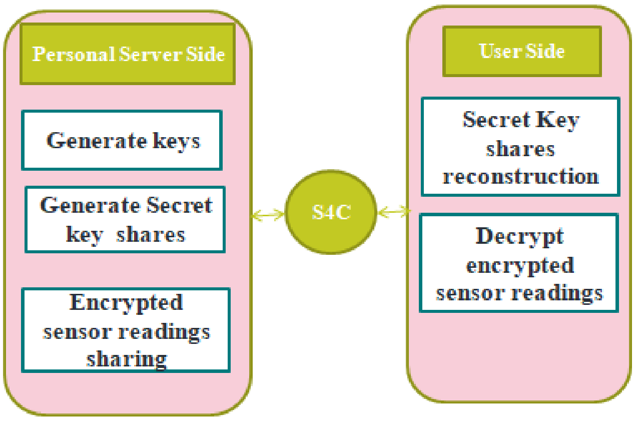

Personal Server Side
Generate keys
Generate Secret key shares
Encrypted sensor readings sharing
S4C
User Side
Secret Key shares reconstruction
Decrypt encrypted sensor readings

Figure 3: Steps involved at the personal server side and user side

5. Results & Discussions

The performance of the suggested S4C algorithm is examined, and the results are discussed. For research investigations, sensor readings derived from random sources are utilized. For experimentation, it assumes eight sensors that are uniformly distributed throughout the human body. These sensors measure human EEG, ECG, blood pressure, heart rate, EMG, and motion level.

Table 1 shows the sensor readings for different transmissions

Transmission ID	EEG (Hz)	ECG (bpm)	Blood Pressure (mm Hg)	Heart rate (bpm)	EMG (microvolts)	Motion1 (degrees)	Motion2 (degrees)	Motion3 (degrees)
Transmission - 1	2.51 Hz	51 bpm	120/73	36	97	2°	6°	8°
Transmission - 2	2.48 Hz	52 bpm	105/78	60	75	32°	16°	9 °
Transmission - 3	1.37 Hz	99 bpm	112/87	44	78	82°	77 °	44 °
Transmission - 4	13.24 Hz	60 bpm	121/81	62	76	28 °	34 °	36 °
Transmission - 5	27.97 Hz	100 bpm	134/72	71	78	46°	20°	61°

Following the acquisition of these sensor readings, they are subsequently transmitted to the Personal Server (PS). To evaluate the cryptography algorithm, a comparison is made between the proposed S4C algorithm and other established cryptography algorithms, including DES [27], AES [28], Blowfish [29], and RC4 [30], under both ECB and CBC modes. Figure 4, 5, 6 and Figure 7 illustrates that the proposed S4C algorithm in ECB mode and CBC mode takes less encryption time and decryption time when compared to DES, AES, Blowfish, and RC4.

Figure 4: Encryption Time Comparison Of Cryptography Algorithms In ECB Mode (in milliseconds)

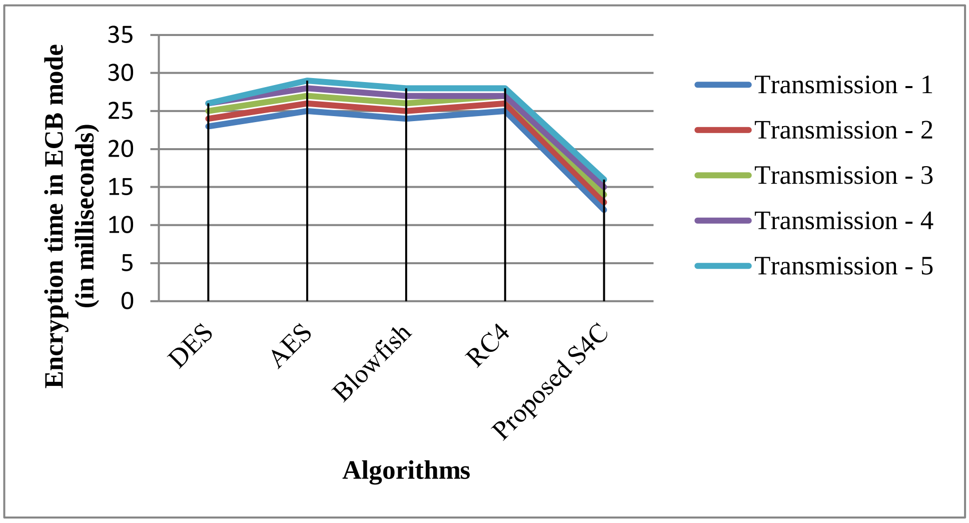


Figure 5: Encryption Time Comparison Of Cryptography Algorithms In CBC Mode (in milliseconds)

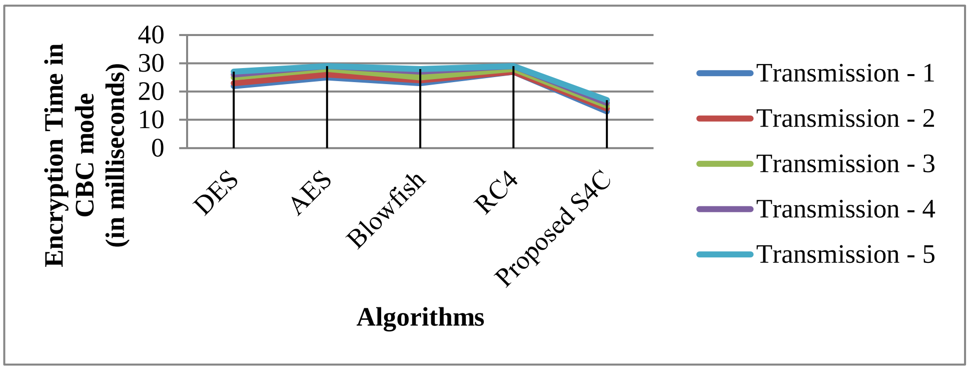


Figure 6:Decryption Time Comparison Of Cryptography Algorithms In ECB Mode (in milliseconds)

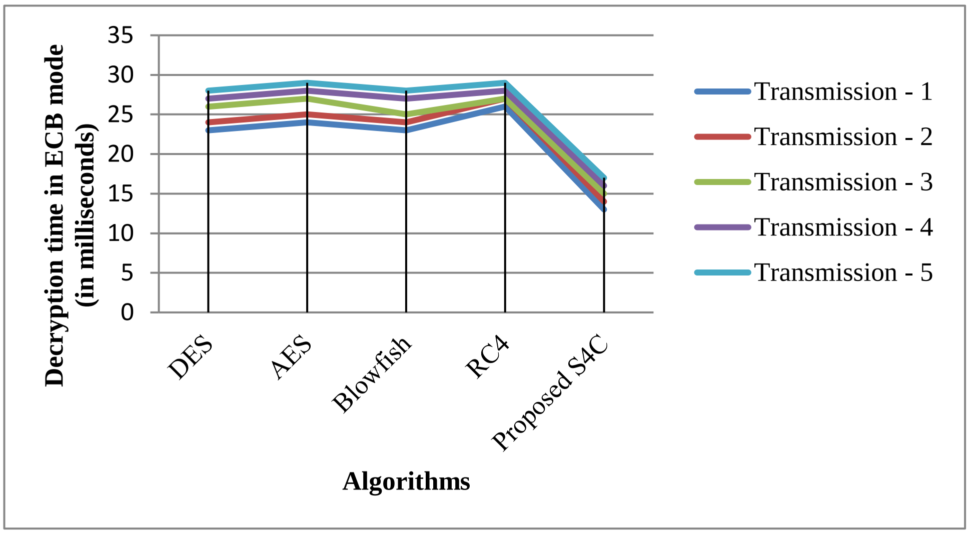
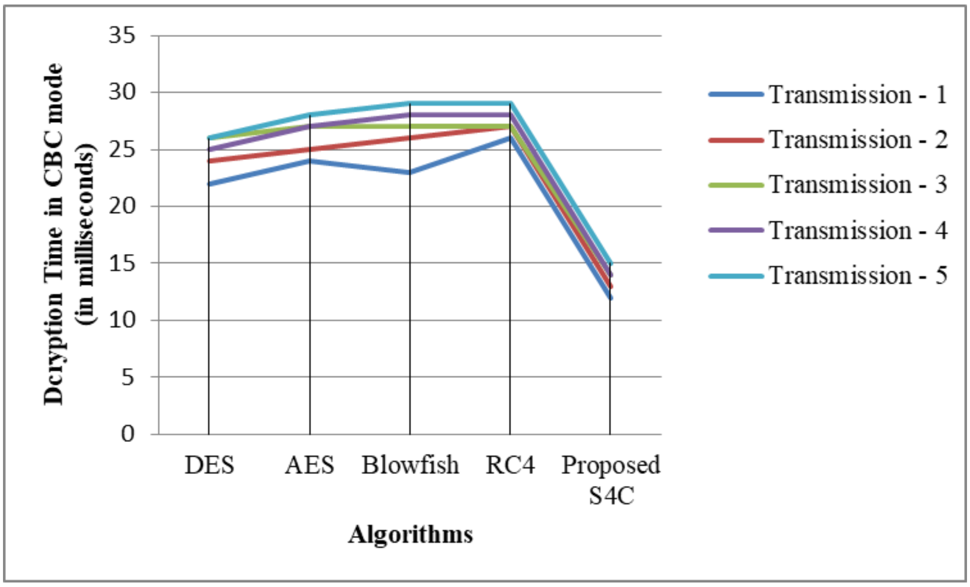


Figure 7:Decryption Time comparison of cryptography algorithms in CBC Mode (in milliseconds)



6. Conclusion

This paper proposes Secure Secret key Sharing based Strong Cryptography (S4C) for secure data transmission in heterogeneous networks. A robust security mechanism with an efficient key generation process, capable of meeting critical data security needs while expediting data encryption, is of paramount importance. In this research, a security algorithm called S4C has been formulated, relying on a streamlined and effective key generation method, coupled with a Secret Sharing procedure. Empirical findings validate that the S4C algorithm offers robust cryptographic capabilities and secure secret key sharing, effectively reducing encryption and decryption time, particularly valuable in healthcare settings operating within heterogeneous network environments.

References

1. M. Al Ameen, J. Liu, K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications", 2012 J Med Syst, 36, pp. 93-101, 2012.
2. B. Pushpa, "Hybrid Data Encryption Algorithm for Secure Medical Data Transmission in Cloud Environment", 2020 IEEE Fourth International Conference on Computing Methodologies and Communication, ISBN: 978-1-7281-4889-2, Mar 2020.
3. H. Peng, Y. Tian, J. Kurths, L. Li, Y. Yang, D. Wang, "Secure and Energy-Efficient Data Transmission System Based on Chaotic Compressive Sensing in Body-to-Body Networks", 2017 IEEE Transactions on Biomedical Circuits and Systems, Volume 11, Issue 3, pp. 558 - 573, May 2017.
4. V. Gupta, G. Metha, "Medical Data Security Using Cryptography", 2018 IEEE 8th International Conference on Cloud Computing, Data Science & Engineering, ISBN: 978-1-5386-1719-9, Jan 2018.
5. H. Huang, T. Gong, N. Ye, R. Wang, Y. Dou, "Private and Secured Medical Data Transmission and Analysis for Wireless Sensing Healthcare System" 2017 IEEE Transactions on Industrial Informatics, Volume 13, Issue 3, pp. 1227 - 1237, Mar 2017.
6. R. Abid, B. Aslam, M. Rizwan, F. Ahmad, M. U. Sattar, "Block-Chain - Security Advancement in Medical Sector for sharing Medical Records", 2019 IEEE International Conference on Innovative Computing, ISBN: 978-1-7281-4682-9, Nov 2019.
7. S. Pirbhulal, W. Wu, G. Li, "A Biometric Security Model for Wearable Healthcare", 2018 IEEE International Conference on Data Mining Workshops, ISBN: 978-1-5386-9288-2, Nov 2018.
8. A. V. Vijayalakshmi, L. Arockiam, "Hybrid security techniques to protect sensitive data in E-healthcare systems", 2018 IEEE International Conference on Smart Systems and Inventive Technology, ISBN: 978-1-5386-5873-4, Dec 2018.
9. W. Fadheel, R. Salih, L. Lilien, "PHeDHA: Protecting Healthcare Data in Health Information Exchanges with Active Data Bundles", 2018 17th IEEE International Conference On Trust, ISBN: 978-1-5386-4388-4, Aug 2018.
10. M. Elhoseny, G. R.González, O. M. A.Elnasr, "Secure Medical Data Transmission Model for IoT-Based Healthcare Systems", 2018 IEEE Access, Volume 6, pp. 20596 - 20608, Mar 2018.
11. M. U. Shaikh, S. A. Ahmad, W. A. W. Adnan, "Investigation of Data Encryption Algorithm for Secured Transmission of Electrocardiograph (ECG) Signal", 2018 IEEE-EMBS Conference on Biomedical Engineering and Sciences, ISBN: 978-1-5386-2471-5, Dec 2018.

12. J. Liu, J. Ma, J. Li, M. Huang, N. Sadiq, Y. Ai, "Robust Watermarking Algorithm for Medical Volume Data in Internet of Medical Things", 2020 IEEE Access, Volume: 8, pp. 93939 - 93961, May 2020.
13. D. Giri, M. S. Obaidat, T. Maitra, "SecHealth: An Efficient Fog Based Sender Initiated Secure Data Transmission of Healthcare Sensors for e-Medical System", 2017 IEEE Global Communications Conference, ISBN: 978-1-5090-5019-2, Dec 2017.
14. N. H. Hussein, "Cloud-Based Efficient and Secure Scheme for Medical Images Storage and Sharing using ECC and SHA-3", 2019 IEEE 2nd Scientific Conference of Computer Sciences, ISBN: 978-1-7281-0761-5, Mar 2019.
15. S. Pirbhulal, W. Wu, G. Li, A. K. Sangaiah, "Medical Information Security for Wearable Body Sensor Networks in Smart Healthcare", 2019 IEEE Consumer Electronics Magazine, Volume 8, Issue 5, pp. 37 - 41, Sep 2019.
16. S. Rajagopalan, S. Janakiraman, A. Rengarajan, "IoT Framework for Secure Medical Image Transmission", 2018 IEEE International Conference on Computer Communication and Informatics, ISBN: 978-1-5386-2238-4, Jan 2018.
17. M. Srivastava, G. Thamilarasu, "MSF: A Comprehensive Security Framework for mHealth Applications", 2019 IEEE 7th International Conference on Future Internet of Things and Cloud Workshops, ISBN: 978-1-7281-4411-5, Aug 2019.
18. A. Ara, M. A.Rodhaan, Y. Tian, A. A.Dhelaan, "A Secure Privacy-Preserving Data Aggregation Scheme Based on Bilinear ElGamal Cryptosystem for Remote Health Monitoring Systems", 2017 IEEE Access, Volume 5, pp. 12601 - 12617, June 2017.
19. V. H. Tutari, B. Das, D. R. Chowdhury, "A Continuous Role-Based Authentication Scheme and Data Transmission Protocol for Implantable Medical Devices", 2019 IEEE Second International Conference on Advanced Computational and Communication Paradigms, ISBN: 978-1-5386-7989-0, Feb 2019.
20. M. M. Hashim, M. S. Taha, A. H. M. Aman, "Securing Medical Data Transmission Systems Based on Integrating Algorithm of Encryption and Steganography", 2019 IEEE 7th International Conference on Mechatronics Engineering, ISBN: 978-1-7281-2971-6, Jan 2020.
21. T.G. Braham, S. Butakov, R. Ruhl, "Reference Security Architecture for Body Area Networks in Healthcare Applications", 2018 IEEE International Conference on Platform Technology and Service, ISBN: 978-1-5386-4710-3, Jan 2018.
22. P.V. Vezeteu, T.A. Capraru, S. Niculae, D.I. Nastac, "Secure Transmission System for Personal Data Acquired Through Optical Character Recognition", 2018 IEEE 24th International Symposium for Design and Technology in Electronic Packaging, ISBN: 978-1-5386-5577-1, Oct 2018.
23. H. Qiu, M. Qiu, G. Memmi, M. Liu, "Secure Health Data Sharing for Medical Cyber-Physical Systems for the Healthcare 4.0", 2020 IEEE Journal of Biomedical and Health Informatics, pp. 1 - 1, Feb 2020.
24. H. Chi, L. Wu, X. Du, Q. Zeng, P. Ratazzi, "e-SAFE: Secure, Efficient and Forensics-Enabled Access to Implantable Medical Devices", 2018 IEEE Conference on Communications and Network Security, ISBN: 978-1-5386-4586-4, Jun 2018.
25. S. Amofa, E. B. Sifah, K.O.B.O. Agyekum, "A Blockchain-based Architecture Framework for Secure Sharing of Personal Health Data", 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services, ISBN: 978-1-5386-4294-8, Sep 2018.

26. M J Vidya, K V Padmaja, "Affirmation of electronic patient record through bio-electric signal for medical data encryption authenticity", 2017 IEEE Region 10 Conference, ISBN: 978-1-5090-1134-6, Nov 2017.
27. K. Q. Aphetsi, M. C. Xenya, "Securing Medical IoT Devices Using Diffie-Hellman and DES Cryptographic Schemes", IEEE 2019 International Conference on Cyber Security and Internet of Things, ISBN: 978-1-7281-7417-4, May 2019.
28. M. Khader, M. Alian, R. Hraiz, S. Almajali, "Simplified AES algorithm for healthcare applications on Internet of Thing", IEEE 2017 8th International Conference on Information Technology, ISBN: 978-1-5090-6332-1, May 2017.
29. S. S. Kondawar, D. H. Gawali, "Blowfish algorithm for patient health monitoring", 2016 International Conference on Inventive Computation Technologies, IEEE 2016 International Conference on Inventive Computation Technologies, ISBN: 978-1-5090-1285-5, Aug 2016.
30. J. Zhang, H. Liu, L. Ni, "A Secure Energy-Saving Communication and Encrypted Storage Model Based on RC4 for EHR", 2020 IEEE Access, Volume 8, pp. 38995 - 39012, Feb 2020.