A Secure WBAN Algorithm using EHC Homomorphic Encryption and Blockchain

Sonam Chourasia[1], Deepak Pathak[2]
[1]MTech Scholar, [2]Assistant Professor,
Department of CSE, RKDF University, Bhopal, M.P, India

* Corresponding Author: Sonam Chourasia

Abstract: *A higher level of network privacy and security is widely identified as a critical aspect of safeguarding this data while used by healthcare professionals as well as during storage to ensure that patient information is protected from attackers. The purpose of this study is to provide a block chain cryptography and bio-informatics validation structure for WBANs deployments. As a result, there is a desperate tendency to use WBANs to address security and privacy issues. WBANs face a wide range of issues. WBAN is a favourite battlefield for cybercriminals due to its adaptability in a wide number of applications. This paper provides a detailed assessment of the major security challenges in WBANs. It is widely understood that a high level of system privacy and security play a critical role in safeguarding this data while used by medical experts, as well as during maintenance to ensure that patient information is protected from hackers. As a result, issues concerning privacy must be addressed in WBANs. An overview of the current state of privacy challenges and potential for WBAN applications is offered, beginning with an examination of the most critical communication links of the WBAN reference implementation and concluding with potential threats and requirements.*

Keywords: *WBANs, EHC, Blockchain, Security*.

I. INTRODUCTION

In today's world, the healthcare system has a huge amount of data. This data is very critical and therefore its security is a major concern. Critical patient health information is conventionally stored in a file and little personal information is stored in the hospital administration database. Hence, the situations that arise when the file is lost are very difficult. To overcome this scenario, a health card is used. This card stores all patient data, including medical reports. Therefore, the security of this data is very important. There are many encryption algorithms to ensure data and network security. Choosing the best of them is very important. As such, a blockchain is inherently encrypted. This property allows data validation. A block in the blockchain represents the available data. Contains information on past and future dates [1].

The blockchain concept is known for its use in Bitcoin and cryptocurrencies. It has received extensive attention from various stakeholders due to its immense business potential and its use in various applications such as banking, healthcare and supply chain management. Medical and health services are one of the most important and crucial services that must be provided in a safe and timely manner. Blockchain as a decentralized and distributed technology can play a key role in providing these health services [2].

II. LITERATURE REVIEW

Park et al. [1] concentrated their study on the development of lightweight authentication and authorization for healthcare IoT applications. The running time of this task was 10ms, and the overall communication overhead was 3008 bits.

Maitra et al. [2] presented a safe verification system with 13ms and 6ms response times, correspondingly. In addition, the suggested algorithm is measured by means of runtime, intricacy, and communication overhead. The processing time has been calculated to be 4ms.

Ramani et al. [3] focused is to design a secure and efficient data accessibility mechanism for current healthcare systems using the blockchain technology. Furthermore, researchers analyzed that the proposed scheme can fulfill the requirements of confidentiality, integrity and authentication. They have also proposed the potential smart contract agreement considering this healthcare scenario.

Christo et al. [4] focused on implementing the elliptic curve cryptography (ECC) technique, a lightTheyight authentication approach to share the data effectively. Many researches are in place to share the data wirelessly, among which this work uses Electronic Medical Card (EMC) to store the healthcare data. The work discusses two important data security issues: data authentication and data confidentiality. To ensure data authentication, the proposed system employs a secure mechanism to encrypt and decrypt the data with a 512-bit key. Data confidentiality is ensured by using the Blockchain ledger technique which allows ethical users to access the data. Finally, the encrypted data is stored on the edge device. The edge computing technology is used to store the medical reports within the edge network to access the data in a very fast manner. An authenticated user can decrypt the data and process the data at optimum speed. After processing, the updated data is stored in the Blockchain and in the cloud server. This proposed method ensures secure maintenance and efficient retrieval of medical data and reports.

Bhattacharya et al. [5] proposed a BC leveraged scheme HeaL for decentralized HIoT-based ecosystems. The scheme proposes a light-Theyight, responsive and resilience based for secure data exchange over WBAN. For the same, nodes elect a local CH responsible for disseminating meta-EHR information to GSN. At GSN, registered healthcare stakeholders execute a lightTheyight sign-cryption scheme, where the keys are fetched from IPFS. The meta-information is verified local miners, and added to local BC ledger. Once, local BC confirms the transaction state, the entries are forwarded to global chain. The obtained results indicate the viability of the proposed scheme against conventional approaches.

Tariq et al. [6] addressed the security requirements of IoT-enabled smart healthcare systems along with the application of blockchain-based security solutions. They dis-cussed how blockchain-based solutions can overcome different security issues in an efficient, distributive, and scalable way. In addition, they also highlighted the challenges of blockchain deployment is this infrastructure. The traditional security mechanisms do not cater for all the security requirements of the IoT-enabled smart health care system due to less scalability, higher cost, single-point-of-failure, and resthece-constrained nature of the IoT devices. Recently, blockchain transpired a new era of security and privacy in the healthcare domain.

Cheng et al. [7] presented a thorough view on the security of blockchain in this work, which facilitates the application in ensuring the security of multimedia content. They first introduce current protection methods of multimedia content and great benefits of combining blockchain and multimedia techniques to improve robustness of the multimedia contents. Though the safety is gaining much more attention than before, the defects in blockchain are yet to be solved completely. In this paper, they describe the basic implementation techniques and working principles of blockchain. Then They describe the security properties provided by the blockchain. This work is centered around the security threats and corresponding countermeasures from the view of the blockchain architecture. In particular, they analyze the strengths and correctness of different methods to protect privacy, as They'll as the related attacks corresponding to each layer of blockchain architecture. They deduce that fairer and more reasonable consensus and incentive mechanisms can be developed based on credit and game theory.

Son et al. [8] proposed a secure protocol for a cloud-assisted TMIS with access control using blockchain. The proposed model utilized the blockchain technology to guarantee data integrity in the cloud server and applied consortium blockchain for scalability and low computation cost. Moreover, They employed CP-ABE for access control of stored data in the cloud so that the proposed model achieved fine-grained access control. Furthermore, the proposed protocol included registration, authentication, data upload, treatment, and checkup. They conducted informal analysis to show that the proposed protocol prevents from a variety of attacks and They compared the security features of the proposed protocol with the related protocols. They also utilized the BAN logic analysis for proving that it supports secure mutual authentication, and AVISPA to show that it is safe for MITM and replay attacks. Furthermore, They compared computation blue and communication costs of the proposed protocol with the

related protocols. They demonstrated that the propose protocol is efficient and has better safety compared to the related protocols. Thus, the proposed protocol is proper for a practical TMIS environment.

Benson et al. [9] not meant to ascertain the efficacy of block chain but to introduce medical professionals to the concept of security with bio-medical devices using block chain. As there exists a preponderance of advanced research topics concerning block chain, the intent of these writers was to focus on the current threat against medical devices and the protection thereof. These authors believe that by exposing the current threats, more medical personnel will embrace and adopt the block chain solution for protection of medical devices and, hence, the protection of the patient. Paramount is the necessity of medical professionals to comprehend the basic principles of block chain and use the information to advance this topic into the medical field. This goal is accomplished through a detailed level of understanding by the biomedical engineer and the medical professionals, with a subsequent outcome of a categorical teaching method to a greater audience of professionals in the medical field.

Internet connected things have very higher growth in near future, i.e., it will be easily adopted by many applications. Together this, vulnerabilities or attacks also be more on IoTs. So, Mishra et al. [10] needed to secure IoTs with efficient and smart solution. Blockchain as decentralized concept, is recognized as a better solution for providing security to data in motion and rest. In this article, they proposed a security mechanism to IoTs based applications/ systems.

III. METHODOLOGY

This process includes three aspects for safe cloud-assisted IOT applications: the user (U), the cloud-service center (CSC), the Authenticator (A), plus blockchain. Before using the technology, each member needs to enroll with the Cloud-Service-Centre, which will provide a unique certification for attempting to access database file in Wireless body area network or Internet of Things. CSC, which is regarded as a legitimate source, initiates the service. The web server maintains health - related information and physician assessment results, as well as uploading data-related operations. A patient submits personalized health information encoded with better attribute-based EHC homomorphic for assessment.

Authenticator will manage the blockchain. Healthcare practitioners and the sufferers can view the blockchain records, and the web server can upload a block of blockchain operations. This study will offer a secure authentication mechanism for a cloud-assisted Wireless Body Area Network that accesses data through blockchain. Authorization control is done using cypher - text attribute-relied encryption (CP-ABE) for medical information stored on the web server, and authenticity is assured using blockchain.

The following stages are included in the proposed protocol:

Step 1: Initiation - All personal and corporate variables are configured in this phase.

Step 2: Verification - The user (U) approaches to the Authenticator to obtain authorization to access or upload a file.

Step 3: Upload Information - The user (U) has the option of uploading a new file or accessing current files. He must supply some accessibility variables in order to access other files, and an accessing license will be granted to the user for a set period of time.

Step 4. The authorized user You have access to files saved in the cloud center.

The initial approach to address safety issues in any industry is the login procedure and associated validation. The procedure of authenticating or verifying that the claimed personality or name seems to be the same and accurate as shown or asserted is known as authenticity. Several techniques for verifying person's authenticity have been presented. Facial biometrics are employed in this investigation. Facial detection is a way for recognizing or authenticating a person's identity by using their face. Patterns are recorded, analysed, and contrasted depending on a person's face features.

After identification and proof of identity, the communication is encrypted for security reasons. Encrypting technique is the act of transforming data into a coded format that is inaccessible by humans and then decrypting it at the receiver's end to make it useable and accessible. Among the encryption algorithms are RSA, Elgamal, homomorphic. EHC homomorphic is also one of the encryption algorithms and is employed in this research project.

IV. RESULTS

The runtime or execution time is approximately calculated as encryption and decryption time. Encryption time or Decryption time is calculated by evaluating the difference between start and stop time.

Table 1: Execution Time Analysis of Proposed Model

	Execution Time (in ms)
Registration	~0.3
Authentication	~2
Encryption	~1
Hash	~8
Decryption	~3

Table 2. Comparative Analysis

Schemes	Execution Time (in ms)	Complexity	Communication Cost
Maitra et al. [1]	~6	$9T_h+8T_{Enc/Dec}$	2432
Park et al. [2]	~10	$20T_h$	3008
Proposed	~4	$8T_h+4T_{Enc/Dec}$	1536

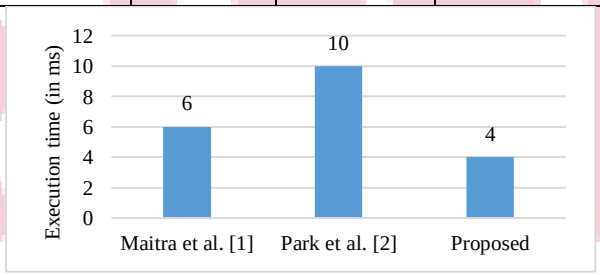

Fig. 1. Comparative Execution Time Analysis

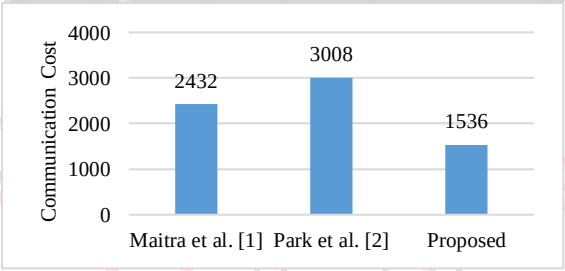

Fig. 2. Comparative Communication Cost Analysis

V. CONCLUSION

In the health world, the Wireless Body Area Network has a great potential. In the WBAN scenario, cyber-security is a big problem. This paper proposes a secure framework to overcome these challenges. In this design, an EHC homomorphic encryption method with attribute-based encrypting technique is employed to provide secure user access that is closely managed. Block-chain is used for its performance and reduced processing cost. As a result, current research work will be targeted in the future more towards the development of a secure block-chain-based system for WBAN.

REFERENCES

[1] Park et al. (2020). LAKS-NVT: Provably Secure and Lightweight Authentication and Key Agreement Scheme Without Verification Table in Medical Internet of Things. IEEE Access, 8,119387-119404. https://doi.org/10.1109/ACCESS.2020.3005592
[2] Tanmoy Maitra, Mohammad S. Obaidat, Debasis Giri, Subrata Dutta, Keshav Dahal, "ElGamal cryptosystem-based secure authentication system for cloud-based IoT applications", IET network, 2019, Vol. 8 Iss. 5, pp. 289-298.
[3] Ramani, V., Kumar, T., Bracken, A., Liyanage, M., & Ylianttila, M. (2018). Secure and Efficient Data Accessibility in Blockchain Based Healthcare Systems. 2018 IEEE Global Communications Conference, GLOBECOM 2018 - Proceedings. https://doi.org/10.1109/GLOCOM.2018.8647221
[4] Christo, M. S., Jesi, V. E., Priyadarsini, U., Anbarasu, V., Venugopal, H., & Karuppiah, M. (2021). Ensuring Improved Security in Medical Data Using ECC and Blockchain Technology with Edge Devices. 2021.
[5] Bhattacharya, P., Mehta, P., Tanwar, S., Obaidat, M. S., & Hsiao, K. F. (2020). HeaL: A blockchain-envisioned signcryption scheme for healthcare IoT ecosystems. Proceedings of the 2020 IEEE International Conference on Communications, Computing, Cybersecurity, and Informatics, CCCI 2020. https://doi.org/10.1109/CCCI49893.2020.9256705
[6] Tariq, N., Qamar, A., Asim, M., & Khan, F. A. (2020). Blockchain and smart healthcare security: A survey. Procedia Computer Science, 175(2019), 615–620. https://doi.org/10.1016/j.procs.2020.07.089
[7] Cheng, J., Xie, L., Tang, X., Xiong, N., & Liu, B. (2021). A survey of security threats and defense on Blockchain. Multimedia Tools and Applications, 80(20), 30623–30652. https://doi.org/10.1007/s11042-020-09368-6
[8] Son, S., Lee, J., Kim, M., Yu, S., Das, A. K., & Park, Y. (2020). Design of secure authentication protocol for cloud-assisted telecare medical information system using blockchain. IEEE Access, 8, 192177–192191. https://doi.org/10.1109/ACCESS.2020.3032680
[9] C. Benson, D. K., Jonassen, D. L., & Tran, D. B. (2019). Cyber security for Medical Devices Using Block chain. International Journal of Applied Science and Technology, 9(4), 10–21. https://doi.org/10.30845/ijast.v9n4p2
[10] Mishra, S. (2019). Based Applications using Blockchain Technolgy. 123–128.