Blockchain Integrated Healthcare Wireless Body Area Network for Security Enhancement

Vipin Panwar
M.Tech Scholar
Department of CSE, NIT, Kurukshetra, Haryana, India
pvipin278@gmail.com

Dr. S. K. Jain
Professor
Department of CSE, NIT, Kurukshetra, Haryana, India

Abstract – A greater standard of network confidentiality and protection is generally accepted as a vital component of securing this data when employed by medical practitioners as well as during storage to guarantee that patient data are maintained safe from intruders. This paper develops block chain cryptography and bio-informatics verification architecture for WBANs implementations. As a result, there is a deep desire to solve security and privacy challenges with WBANs. WBANs confront a wide range of problems. Because of its versatility in a wide range of applications, WBAN is a favoured battleground for cybercriminals. This work also provides a blockchain integrity check and bio-informatics authentication framework for WBANs implementations. Hence there is an important interest to address security and privacy problems in WBANs.

Keywords – Wireless Body Area Network, Security Issues, Encryption, Blockchain, Biometric Authentication.

I. INTRODUCTION

A body area network (BAN) is a network of wireless sensors mounted in, on and across the body that is short-range. It offers short distance data communication, limited to a few metres range. The basic concept is shown in figure 1 below. This new network type uses electronically implanted and wearable circuits. It performs really useful duties and features in pleasant, discrete designs that consume extremely little energy and provide absolutely exceptional safety [1]-[5].

The sensor nodes are located directly on or under the person's body to measure such parameters such as, body activity, electrical cardiogram (ECG), temperature, blood glucose, blood pressure, biosensor, pulse rate and breathing rate speeds. The sensor nodes are mounted directly under or at the body. These sensors are designed to satisfy the specifications of ends for particular purposes. An EEG tracker, for instance, was intended for brain electric activity control. Another example is the ECG sensor developed for cardiac activity control [6]-[7].

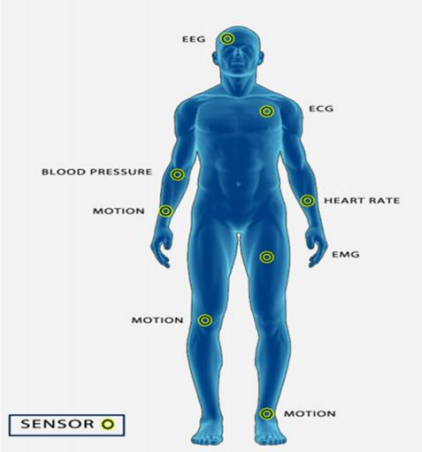

Figure 1 : WBAN sensors

The location of the sensors interacting via a WBAN is normally seen in Figure 1. It can also be used in a range of other areas and technologies such as emissions monitoring, physiological and wellbeing monitoring, contact with human machine, education and entertainment.

A. Various Utility of WBAN in Health Monitoring

WBAN collects health data from the observed bodily state using a network of biological sensors. Conditional reactions to a health issue are provided by the synchronization of sensors and actuators. For instance, in high blood sugar control, tiny actuators for insulin administration are used [8]-[10]. Wireless body sensors comprise transducers for signal analysis, a power source, and transmitter and receiver circuitry for wireless connections. WBAN measures and transmits important information to remote health units over wireless media using battery-powered wireless biological sensors. WBAN devices are difficult to replace due to the minor dimension of the sensors. Similarly, its battery's endurance is determined by its size. As a result, WBAN's operating lifetime is jeopardised by a smaller battery. WBANs face blockage and other media barriers whenever operating near similar gadgets in much the same radio frequency spectrum, such as ZigBee and WiFi

coexistence inside the ISM band or conflicting frequencies in the data transmission. (2.4 GHz).

B. WBAN architecture

WBAN consists of smart objects that are connected via a computer processor. Sensors monitor genetic differences including blood glucose, warmth, insulin, ECG, EEG, and other important signs of the body, while controllers answer to the command depending on the sensor measurement [11][12]. In diabetes patients, the transducer, for example, controls blood glucose by regulating insulin sensitivity. Invasive and non-invasive techniques, including such skin interactions or wearable devices, can be used to embed WBAN sensors in or on the body. WBAN gadgets can only broadcast and receive signals within the limits of the human body.

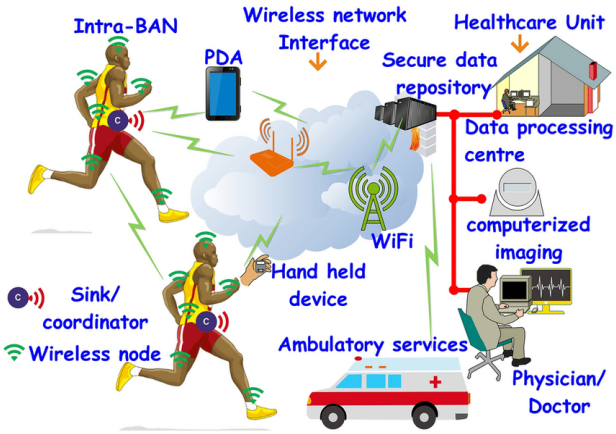

Figure 2: WBAN and beyond WBAN architecture

II. LITERATURE REVIEW

Maitra et al.[1] came up with system termed as an ElGamal cryptosystem and also the biometric information which together with authentication scheme depend on person's password for the program process which is totally on the basis of cloud IoT program can also be called as SAS cloud. The detail finding about SAS cloud also concludes the high level efficient performance over other rivals such as authentication ways depending on ElGamal cryptosystem.

Another recommendation of Son et al. [2] with a safer authentication protocol for helping over cloud TMIS accompanied by entrance security through blockchains. To set up entrance security for wellness of data retained over cloud server the policy named as ciphertext-policy attribute-based encryption (CP-ABE) is adopted and employed blockchain also that to impart assurance of integrity of data.he presentation after research says that this scheme of suggestive protocol gives huge safety and also level up capability than to linked other protocols. In feasible TMIS surrounding the recommendation is suitable.

Li et.al in [3]To address IoMT's privacy, security, and interoperability concerns. By adding blockchain to existing IoMT systems, researchers provide a framework for blockchain-enabled IoMT. In this article, researchers go over the advantages of this architecture and show how blockchain-enabled IoMT can benefit businesses. Researchers also discuss how blockchain-enabled IoMT can be used to combat the COVID-19 pandemic, including infectious disease prevention, location sharing and contact tracing, and injectable drug supply chain management.

Sangari et al. [4] have developed a lightresearchersight public key crypto framework for wireless body sensor network security as researchersll as the experimental results of the proposed bio sensor node scheme that demonstrates our system's effectiveness in practise.

A new and stable diverse ticket-sales system (DTS) is proposed by Chang et al. [5] in hybrid cloud utilizing smart cards. In accordance with the BAN logic, the accuracy of participant authentication involved is demonstrated. The DTS has a ticket integration platform where services providers can delegate to the centralized server the selling of their service tickets, and clients can freely navigate to the system and buy e-service tickets at any networked venue.

Cheng et al. [6] have proposed an ordered-Physiological-Feature-based Key Agreement, or OPFKA, is a new key solution that enables a symmetrical cryptographic key generated from intersecting physiological signal features and functionality to also be acknowledged by motion sensor pertaining to the very same BAN, ignoring the previous allocation of key material among sensors installed inside the body.

Pawar & Kalbande [7] conducted a systematic review on wireless body area data security and a review of literature on using block-chain techniques in wireless body area networks, and researchers discovered that there is a requirement to establish secure algorithms using the dynamic nature of block-chain technology in conjunction with optimum Qos metrics.

Zhou et al. [8] proposed a safe and confidentiality key management system for cloud-assisted WBANs that is resistant to mobile assaults in m-healthcare social networking sites. It considerably expands the based on the dynamics of the prior projects to a more realistic context in which the sufferers are permitted to function as common citizens outside and are subjected to a variety of advanced attacks. The paper then provides formal definitions of time-based and location-based mobile sensing compromising threats, suggests matching constructs, and demonstrates their safety and confidentiality

Deng et al. [11] proposed a design for constructing a cloud server layer in WBANs utilizing block-chain based. Each hub node of the cloud server tier stores one personal block-chain. The private block-chain is in charge of

capturing the sensor node and hub node enrollment data. The sensor node collects the patient's physiological parameters, which is then kept by the health care facility. The decentralized storing of identification and physiologic information can significantly reduce system complexity. The adding of new blocks to the block-chain is accomplished by the system's exposed to light, which ensures the block-chain's openness.

Table 1: Comparative Analysis of Existing Techniques

Author	Algorithm Used	Complexity
[1]	ElGamal	$T_{exp}+7T_h+T_m$
[14]	SHA-256 hash functions and bitwise XOR operations	$16T_h$
[15]	AES	$17T_h$
[16]	ECC	$4T_m + 11T_h$

III. METHODOLOGY

Three roles are involved in a secure cloud-assisted IoT platform: the Cloud service centre (CSC), the user (U), the Authenticator (A), and the blockchain. Before using the platform, each user first must enroll with CSC, which will then provide a unique certification that allows them to access WBAN/IOT data sets. The blockchain entries can be accessed by patients and clinicians, and the researchersb server can post block of transactions of blockchain.

The proposed protocol includes following steps:

- **Step 1. Initialization.** In this step all public and private parameters are initialized.
- **Step 2. Authentication.** The participant U approaches to the Identity provider to get accessibility to or upload a document that requires authentication.
- **Step 3**: **Upload the data** U has the option of uploading a new file or accessing current files. He must give certain accessibility criteria in able to reach other files, and an access licence will be granted to the user for a set period of time.
- **Step 4**: The authorised user U has access to the cloud center's documents.

Security Blockchain

Blockchain has already proven its worth in the healthcare and life sciences industries by facilitating trust and collaboration. Blockchain can assist address difficulties in the healthcare and life sciences industries by offering faster access to reliable information, enabling secure permissioned data exchange across various stakeholders, boosting cooperation, and increasing transparency.

Besides the above technical methodologies and techniques used in this study for security. Another major role is played by Data centre. The data centre which resides at the cloud. This database is used to store the cryptographic keys of user. Once the key are created and stored, then each and every time whenever access is required these keys will be compared to check and validate the authenticity and authorization of the message for message delivery ensuring the security. So it is necessary to use secured database and data centre to make this research work more effective and promising. Here in this study cloud storage is opted.

IV. RESULT ANALYSIS

A. *Screenshots of Implementation*

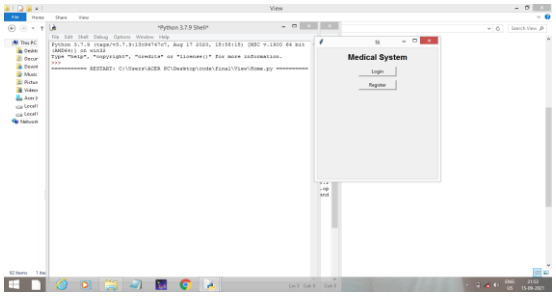

Figure 3: Home Page Frame

This frame is designed to register face biometrics of the user and save in database as illustrated in figure 3. Along with face biometrics, password is also saved for authentication of user for further communications. User can be patient or doctor. Individual logins are presented here for both.

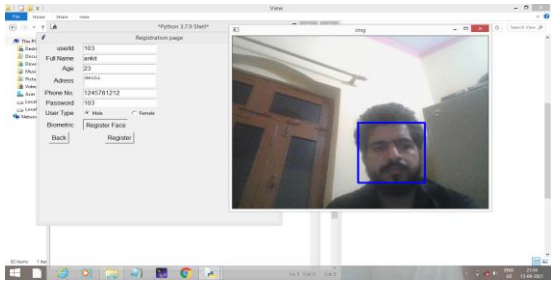

Figure 4. User Registration Frame

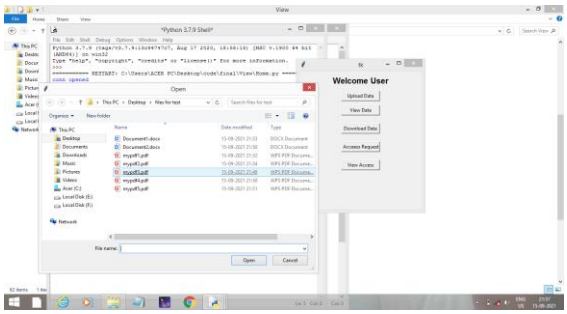

Figure 5: User Dashboard Frame

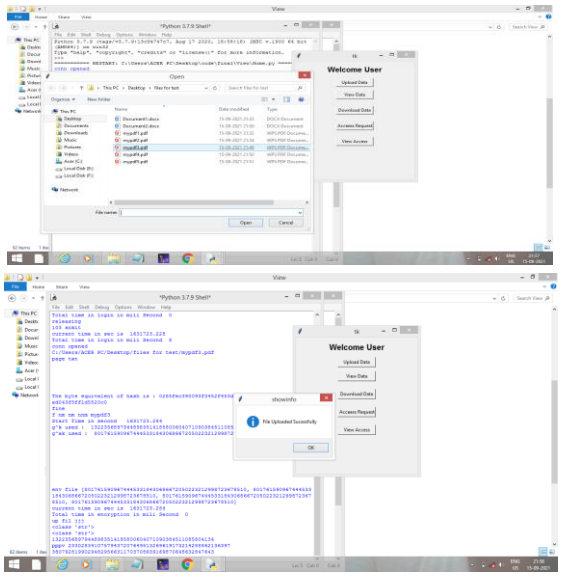

Figure 6: File Uploading Frame

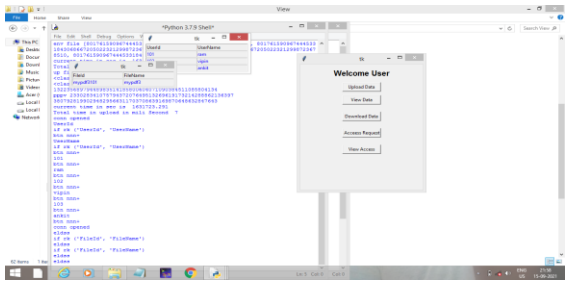

Figure 7: User List with Their Respective File Lists Frame

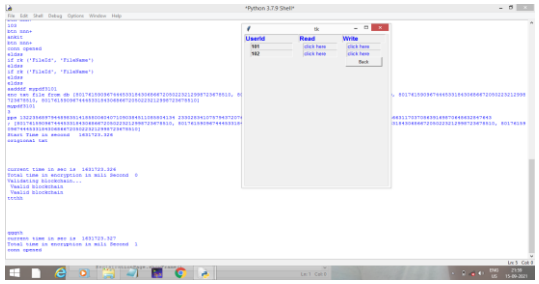

Figure 8: File Accessing Frame

Figure 9: Encryption Time

B. Comparative Performance Analysis

The runtime or execution time is approximately calculated as encryption and decryption time. Encryption time or Decryption time is calculated by evaluating the difference betresearchersen start and stop time. Table 2 gives estimated time essential to run the application. Likewise, in fig 10 and 11, performance by comparing to existing works.

Table 2: Analysis of the Proposed Model's

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

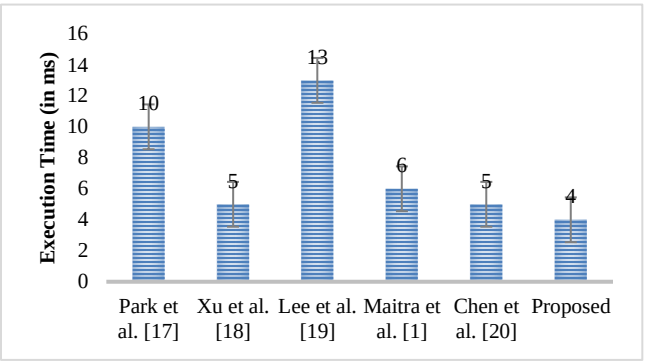

Figure 10: Execution Time (in ms) graph for different work.

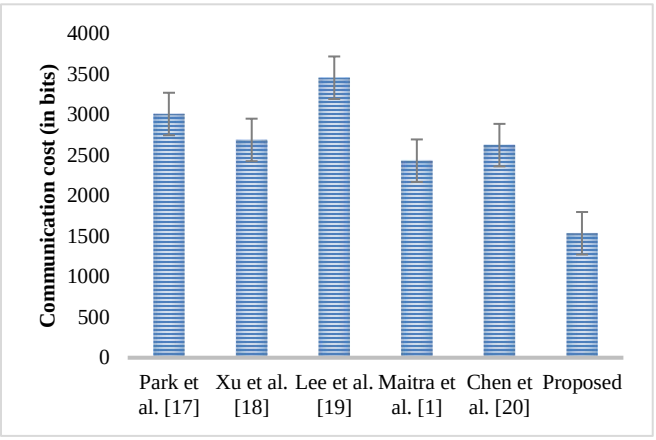

Figure 11: Analysis of Communication Costs Comparison

V. CONCLUSION

In the WBAN scenario, Cyber threat is a key problem. This paper proposes a robust architecture to solve these problems. Elgamal encryption scheme with attribute-based encryption used in this architecture to offer safe user access and to strictly regulated. Block-chain is implemented for flexibility and cheap computational complexity. As a result, present study activities will be directed in the upcoming toward the creation of a safe block-chain-based infrastructure for WBAN. By

evaluating the primary vulnerabilities of each of the specified communication levels in the WBAN reference implementation, the state-of-the-art of safety issues as researchersll as opportunities for WBAN applications in medical setting is present

REFERENCES

[1] 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.

[2] S. Son, J. Lee, M. Kim, S. Yu, A. K. Das and Y. Park, "Design of Secure Authentication Protocol for Cloud-Assisted Telecare Medical Information System Using Blockchain," in IEEE Access, vol. 8, pp. 192177-192191, 2020, doi: 10.1109/ACCESS.2020.3032680.

[3] X. Li, B. Tao, H. N. Dai, M. Imran, D. Wan, and D. Li, "Is blockchain for Internet of Medical Things a panacea for COVID-19 pandemic?," Pervasive Mob. Comput., vol. 75, p. 101434, Aug. 2021, doi: 10.1016/J.PMCJ.2021.101434.

[4] A. Siva Sangari, J. Martin Leo Manickam, "Public key cryptosystem based security in wireless body area network", International Conference on Circuits, Poresearchersr and Computing Technologies, 2014.

[5] C. Chang and T. Cheng, "A Secure Diverse Ticket-Sale System in a Distributed Cloud Environment," in The Computer Journal, vol. 57, no. 10, pp. 1441-1459, Oct. 2014.

[6] C. Hu, X. Cheng, F. Zhang, D. Wu, X. Liao and D. Chen, "OPFKA: Secure and efficient Ordered-Physiological-Feature-based key agreement for wireless Body Area Networks," 2013 Proceedings IEEE INFOCOM, Turin, 2013, pp. 2274-2282.

[7] Pawar, R., & Kalbande, D. (2020). Use of blockchain technology in wireless body area networks. Proceedings of the 3rd International Conference on Intelligent Sustainable Systems, ICISS 2020, 1333–1336. https://doi.org/10.1109/ICISS49785.2020.9316005

[8] Zhou, J., Cao, Z., Dong, X., Xiong, N., & Vasilakos, A. V. (2015). 4S: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks. Information Sciences, 314(September) 255–276. https://doi.org/10.1016/j.ins.2014.09.003

[9] Xu, J., Meng, X., Liang, W., Zhou, H., & Li, K. C. (2020). A secure mutual authentication scheme of blockchain-based in WBANs. China Communications, 17(9), 34–49. https://doi.org/10.23919/JCC.2020.09.004

[10] Rifi, N., Rachkidi, E., Agoulmine, N., & Taher, N. C. (2018). Towards using blockchain technology for IoT data access protection. 2017 IEEE 17th International Conference on Ubiquitous Wireless Broadband, ICUWB 2017 - Proceedings, 2018-January, 1–5. https://doi.org/10.1109/ICUWB.2017.8251003

[11] Deng, H., Meng, X., Guo, J., Xi, E., & Zhao, H. (2020). A Framework of Blockchain-Based Security for WBANs. Proceedings - 2020 3rd International Conference on Smart BlockChain, SmartBlock 2020, 75–80. https://doi.org/10.1109/SmartBlock52591.2020.00021

[12] Mohammed Dakhel and Soukaena Hassan, "A Secure Wireless Body Area Network for E-Health Application Using Blockchain", Applied Computing to Support Industry: Innovation and Technology. Communications in Computer and Information Science, vol 1174, pp. 395–408, 2020.

[13] J. Xu, X. Meng, W. Liang, H. Zhou and K. -C. Li, "A secure mutual authentication scheme of blockchain-based in WBANs," in China Communications, vol. 17, no. 9, pp. 34-49, Sept. 2020, doi: 10.23919/JCC.2020.09.004.

[14] Bhawna Narwal and Aman kumar Malhotra, "SAMAKA: Secure and Anonymous Mutual Authentication and Key Agreement Scheme for Wireless Body Area Networks" Arabian journal For Science and engineering, 2021.

[15] B. Krishna, P. Rajkumar, and V. Velde, "Integration of blockchain technology for security and privacy in internet of things," Mater. Today Proc., Feb. 2021, doi: 10.1016/J.MATPR.2021.01.606.

[16] Shanthapriya.R, Vaithianathan.V, "ECG-Based Secure Healthcare Monitoring System in Body Area Networks", International Conference on Biosignals, Images and Instrumentation (ICBSII), 2018.

[17] K. 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

[18] Xu, Z., Xu, C., Liang, W., Xu, J., & Chen, H. (2019). A lightweight mutual authentication and key agreement scheme for medical internet of things. IEEE Access, 7, 53922–53931. https://doi.org/10.1109/ACCESS.2019.2912870

[19] Xu, Z., Xu, C., Chen, H., & Yang, F. (2019). A lightweight anonymous mutual authentication and key agreement scheme for WBAN. Concurrency and Computation: Practice and Experience, 31(14), e5295. https://doi.org/10.1002/cpe.5295

[20] C. Hu, X. Cheng, F. Zhang, D. Wu, X. Liao and D. Chen, "OPFKA: Secure and efficient Ordered-Physiological-Feature-based key agreement for wireless Body Area Networks," 2013 Proceedings IEEE INFOCOM, Turin, 2013, pp. 2274-2282.