Journal of Computing, Science &Technology
https://focjournal.unidel.edu.ng/
editorjcst@unidel.edu.ng
ISSN:.....Print
ISSN: ..... Online

Theoretical Review of Ethereum Blockchain Based Internet of Medical Things (IoMT) System in the 21st Century

Okeh O. D.[1] & Emuobonuvie, E. A. [2] Anazia E.K[3] & Agbaje, M. O. [4]
[1,2]Department of Computer Science, Faculty of Computing, University of Delta, Agbor,
[3]Department of Information Systems, Faculty of Computing, Delta State University of Science and Technology, Ozoro, Delta State, Nigeria, [4]Department of Computer Science, Babcock University, Ogun State.
dono.okeh@unidel.edu.ng[1], andy.emuobonuvie@unidel.edu.ng[2], Kaynmax07@yahoo.com[3], agbajem@babcock.edu.ng[4]

Corresponding Author's Email: dono.okeh@unidel.edu.ng

Article Info

Date Received: 15-03-2024
Date Accepted: 04-05-2024

Keywords:
Security, Internet of Medical Things (IoMT), Telemedicine, Wearable sensor

ABSTRACT

The interconnectivity of digital devices has made tremendous impact in the lives of individuals, corporate organizations and institutions alike in recent times. The impact experienced by this great technology has attracted the attention of hoodlums posing as hackers obstructing the activities of the Internet. The health sector which parades vital data of patient cannot afford to be exposed freely to these unlawful users of the Internet. Patients' health records should be protected hence this paper has proposed a secured medical system to take care of patient's data which have gained entrance into cloud computing and are stored on the cloud alongside the ones in transit. The paper looked at the taxonomy of the Internet of Things layer-wise and the taxonomy of security protocols used by the layers respectively. Finally, a blockchain methodology using Ethereum technology was proposed.

1.0 INTRODUCTION

The internet of things (IoT) is geared towards connecting things, computers and people across different continents and providing them with different kind of services The process involves the transmission of data and information from one point to another while using some kind of telecommunication technologies. Monitoring systems interact in an intelligent medical system. The process involves wearable devices emanating from the use of IoT. These health monitoring devices enables instruments interact with the network and as such track the data that are involved [1, 2]. It has been established that one of the most formidable technologies in the health sector is telemedicine. This field involves the interaction of medical experts and patients irrespective of distance and time.

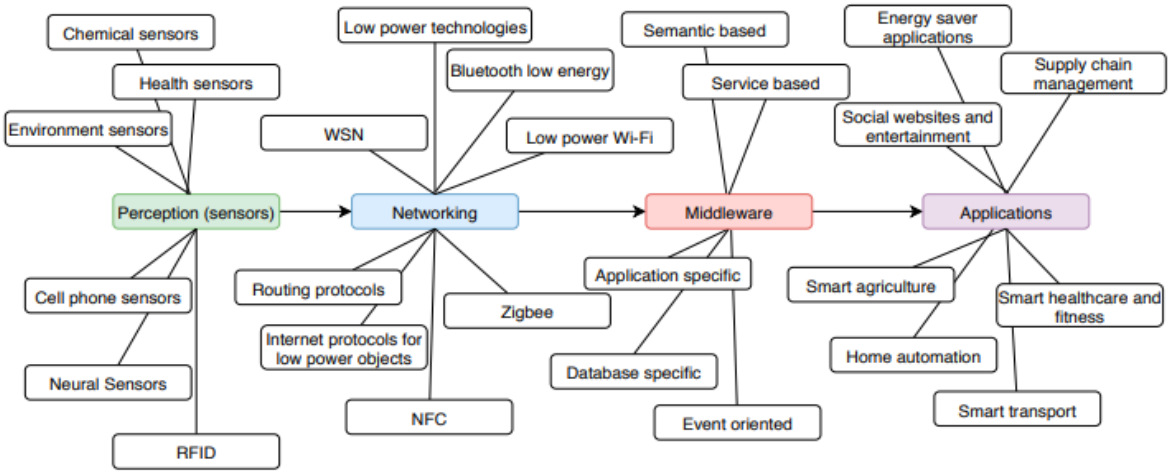

Fig 1: Research taxonomy of Internet of Things (layered-wise)

Patients can receive consultations from remote experts atanytime and anywhere [3,4]. IoT technology has revolutionized the medical industry. Patients can now discuss with medical experts and their health condition monitored remotely. This technology cannot be compared to the traditional method which involves manual collection of data. It is observed that the wireless body sensor network demonstrates good and accommodatable outcome [5]. A miniaturized electronic device for collecting useful data in the health sector are termed "Wearable sensors". These devices in field of medicine are used in acquiring physiological information. They make use of sensor nodes in the transmission of these information to remote sites using multi-hop technology. IoT-based remote wearable devices are used for the monitoring of patients. However, the collected data from patients through the use of wearable devices are private. This calls for the authentication of the entire system which forms the basis for secure communication among devices. To this end, the captured data are sensitive and deserved special protection. If transmitted using plain text and without proper access control will violate user's privacy. The consequences of such act will be catastrophic.

2.0 IoT Architecture and Protocols

Internet of Things has different standard which has been proposed by different researchers at different instances. As long as no universally accepted architecture for Internet of Things have been put in place, different architectural designs are supported by a given set of protocols.

2.1. The Architectural Layer Design: Figure 1, illustrates the three layer architecture layer which was used at the beginning of IoT [7, 6]. Moreover, a more robust architecture having four layers have been developed [8]. These levels of layers are the perception, network, middleware and the application respectively. These different layers are meant to ascertain different operations geared towards perfect service

2.1.1. Perception layer

This is the closest layer to the users of the system. This is primarily designed to interact with the user. The perception layer deals with real physical Internet of Things devices, The internet of things devices in this layer cut across sensors, actuators, and other internet enabled components. The primary responsibility of this layer lies in its ability to sense the environment and capture data. Different types of internet attacks are detected in the process: spoofing, phishing, eavesdropping, and other forms of data breaches are likely.

2.1.2. Network layer

This layer is next to the perception layer in the architecture of the Internet of Things. It takes care of communications between Internet endpoints and servers. Information delivered by the perception layer is subjected to critical analysis. Activities involving data breaches such as phishing, Denial of Service (DoS) or Distributed Denial of Service (DDoS) and other distinctive attacks are analyzed in this layer [10, 11, 9].

2.1.3. Middleware layer

The primary aim of the middleware layer is to enable communication between the first and second layers. The middleware layer carries out the processing duty. It serves dual purpose of storage facility and a computing environment. This layer is involved in several activities such as determining the storage of data as well as the queuing system. It is also engaged in machine learning. In spite of the necessity and sensitivity of this layer in delivering reliable IoT application, it is also disposed to various attacks.

2.1.4. Application layer

The application layer marks the end architectural stages of the respective layers. Most of the Internet of Things use cases (smart cities, smart homes, smart grids, healthcare), and many more, are defined at the application layer. Security breaches such as data theft, privacy invasion, are all components discussed in this layer. The major goal of this layer is to stop the activities geared towards data theft.

2.2. Protocols

Protocols are set of rules that governs the flow of communication in a network. Figure 2 depicts the various protocols that appear at IoT system layers. Internet of Things (IoT) communication systems in most cases have unique protocols. Although some are similar in the case of traditional IT systems. The following protocol are established in the Internet of Things: IEEE 802.15.4, NFC, ZigBee, BLE.

3.0 IoT Environment Security Requirements

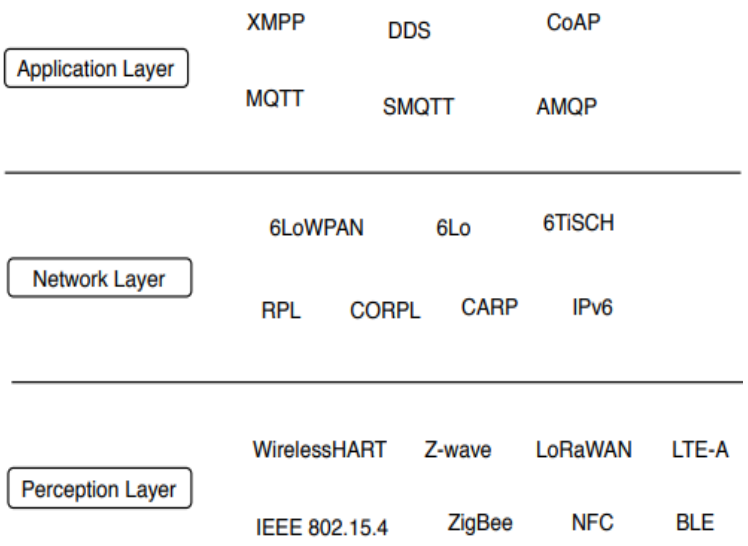

Fig 2: IoT protocols at each layer
Source: Procedia Computer Science

In a networked system, security requirements are needed to ensure its safety. Security measures are needed for the proper functioning of wireless sensors usage in the IoT network. As such, an IoT network needs essential security requirements for it to function properly in a secure environment. These requirements are stated below:

- Authentication: Sensing devices stand at the point of authentication. Every user of a system goes through authentication process before having access to resources. Authentication encompasses sensing devices, users and gateway nodes.
- Integrity: This means that the properties of an object must remain the same. Transmitted data should retain the form with which they are transmitted.
- Confidentiality: Unauthorized disclosure is never allowed at any instance. Unauthorized disclosure of information is hidden. This establishes privacy of the wireless communication channel.
- Availability: Authorized users of the network should have access to the network devices and services at the need time that information is being requested.
- Non-repudiation: Inability of mischievous entity from hiding his/her actions.
- Authorization: Only users who are given legitimate right can make use of the IoT sensing devices.
- Freshness: It drives the affirmation of new information while the old ones are completely discarded.
- Backward secrecy: Newly added IoT sensing node should not possess the ability of reading previously transmitted messages.
- Replay attack: This kind of attack creates a scenario whereby a fraudster redirects an information sent to another authorized entity and in the process reuses the transmitted information. The transmitted information is placed under record by the third party in this type of attack.
- Man-in-the-middle attack: As the name implies, the attacker possess to be at the middle and intercepts the transmitted messages with the intention of altering it. He carries out actions capable of altering the content of the messages delivered to the recipients. This includes actions such as insert/delete which modifies the contents of the messages delivered to the recipients.
- Many logged-in users with the same login-id attack: A table verifier table that checks the user log-in details is created. This looks into the users password and verifies if he is a legitimate user before giving permission. The system can be subjected to many logged-in users with the same login-id attack. Therefore, the system should be able to guide the login details of different entities trying to get access into the system
- Stolen-verifier attack: This kind of attack allows the hacker to retrieve a potential user's documents. Credentials such as log-in details and password are stolen from a stored password table. In designing the security protocols of Internet of Things verifier/password table for verification should not be stored permanently. Storage of verifier or password table can only be put in place when there exist strong and resilient protocols that can defend such type of attack.
- Stolen/lost smart card attack: Attackers are capable of extracting information from smart card that is stolen or gotten without the owner's concept. The information stored in the smart card can be retrieved power analysis attacks technique [12]. Therefore, security protocol in IoT should be designed with restriction on a third party who intends to manipulate smart card that is stolen/lost,
- Password guessing attack: Eavesdropped messages and stored information are used by fraudsters to guess a legitimate registered user by using this kind of attack in the system.
- Password change attack: This attacking type is used by fraudster to alter the password of an authorized registered user.
- Denial-of-Service attack: A DoS attack occurs based on the activation of many factors. These factors include factors associated with the environment or resource depletion, errors from software and hardware as well. [13].
- Privileged-insider attack: Such attacking techniques is employed by a privileged member of the organization. This gives a trusted user within the organization the privilege to attack while in the system. To this regard, the security protocols designed for IoT environment should stop anyone who tries to compromise the system.
- Impersonation attack: Impersonation attack is used by fraudster in such a way that he tries altering fake messages in order to defraud legitimate users in a network on behalf of a sending entity. The receiver of the message is made to believe that the message was sent by an authorized entity.
- Resilience against sensing device capture attack: This attack allows extracted information stored in captured sensing devices to be compromised during the process of communication between other non-compromised sensing devices. Because In IoT environment, the IoT sensing devices are not under protection by any physical means. Hence the sensing devices are prone to attackers in the process of physical capturing.

4.0 Proposed Methodology

The IoT processes in involved in the storage of data in the traditional method is to store all data on the cloud. These stored data are exposed to anyone who uses the cloud and as such there should be security measures put in place to safeguard these data. It is necessary that users should be aware of persons authorized to get access to

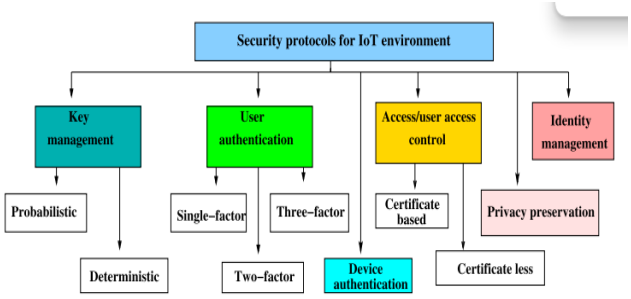

Fig 3: Taxonomy of security protocols in the IoT environment

their information. This is simple reason prompted the methodological approach understudy. A system with robust security features is hereby proposed to handle patients' data that are stored using cloud computing. Sensitive data are not expected to be exposed to the hands of hoodlums parading the Internet. Appropriate control and measures are needed to handle these sensitive data. Considering the security approach in this direction, a well-known technology (Blockchain technology) is proposed for the deployment. This will in turn need to the actualization of this system. Blockchain has a lot of varieties that are currently available in the computing industry but Ethereum has been proposed for this study based on its excellent and magnificent security standards. Two fundamental reasons call for the use of Ethereum technology:

1. Ethereum has over the years gotten the confidence from its end users. Establishments that have deployed its service tagged it to be trustworthy and claiming its safe and secure.
2. Ethereum can easily store its data in a decentralized manner and it is excellent for employing smart contracts. Doctors easily make use this smart contract to keep clear track of their patients.

4.1. System's proposed algorithm

This section presents the proposed blockchain approach algorithm depicting the step by step approach on how it works. These action are demonstrated with the following steps:.

1. Create an Ethereum account for each patient/user.
2. Create a blockchain for storage.
3. Deploy IoT nodes on surroundings.
4. Encrypt sensor values.
5. Store data on Mater node cloud database.
6. Do data preprocessing.
7. Upload cloud address to a patient block.
8. Invite a doctor.
9. Doctor decrypt the encrypted data with his private key;
10. Doctor gives advice and suggestions on the patient block.
11. Terminate the process after a stipulated time,

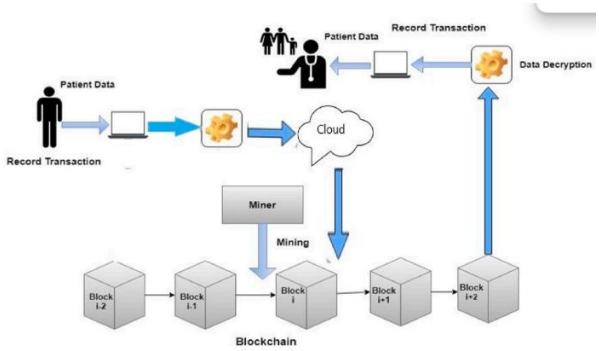

Figure 4: The overview of blockchain based e-health system
Source: Measurement: Sensor 25(2023)

Fig. 4 shows the two parts (the IoT and blockchain) of the proposed system. Encrypted data captured through the use of sensor data are secured and saved in the cloud using cloud technology. The blockchain keeps track of the cloud address.

4.2. The System's Model

We modeled the system representation in such a way that allows for remote patient monitoring. This technique establishes security against data breaches. The idea that patients' data could be easily altered by malicious users. The researchers are with the intention of creating a safe and trustworthy platform for patients. The steps employed in building the platform are as follows:

i. IoT Access Points (Data nodes).
The IoT access points capture the patient's sensible data using varieties of sensors.

ii. Blockchain creation.
A blockchain creation for each patient in an Ethereum network. Modification carried out on a block content in the blockchain network automatically alters all blocks that were created before it. So, any update in the network in respect of patient's data adjusts every other node. [14,15].

iii. Doctor permission.
A doctor in the system is given permission to access the patients blocks. In a like manner, a patient has the right to give a trusted doctor access to his/her block data. Within a time frame, a doctor with a valid Ethereum account can read/write to a patient block when given permission by the patient. To this end, the

doctor uses his private key to decrypt the data sent to him.

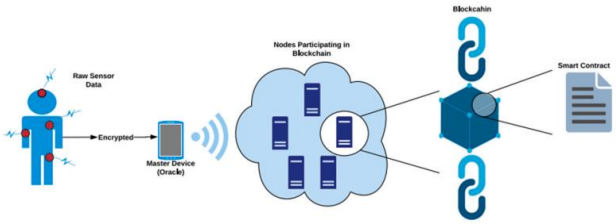

Figure 5: System Architecture Source: Measurement: Sensor 25(2023)

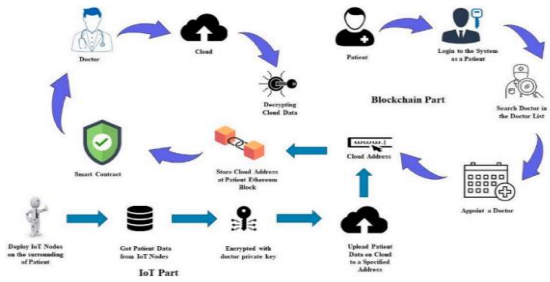

Fig 6: Flow diagram of Proposed Methodology Source: Measurement: Sensor 25(2023)

5.0 Conclusion

IoT technology has revolutionized the medical industry. Patients can now discuss with medical experts and their health condition monitored remotely. This is a welcome development in the health sector. The traditional method is gradually fading away with this new innovation. Patients are no longer expected to queue while waiting endlessly to be attended to by a doctor. The use of sensor devices in gathering data through the wireless body sensor network shows more obvious advantages. The implementation of this proposed methodology will surely go a long way in alleviating the suffering of patients in getting doctors attention.

6.0 References

[1] M. Kang, E. Park, B.H. Cho, et al., Recent patient health monitoring platforms incorporating internet of things-enabled smart devices[J], Int. Neurourol. J. 22 (Suppl 2) (2018) S76.

[2] P. Sundaravadivel, E. Kougianos, S.P. Mohanty, et al., Everything you wanted to know about smart health care: evaluating the different technologies and components of the internet of things for better health[J], IEEE Con.r Electron. Mag. 7 (1) (2017) 18–28.

[3] X. Zhang, J. Sun, C. Li, Development and research of exercise heart rate monitoring system under the concept of Internet of things telemedicine and mobile health[J], J. Med. Imag. Health Inform. 11 (4) (2021) 1106–1111.

[4] A. Azizy, M. Fayaz, M. Agirbasli, Do not forget Afghanistan in times of COVID-19: telemedicine and the Internet of things to strengthen planetary health systems[J, OMICS A J. Integr. Biol. 24 (6) (2020) 311–313.

[5] G. Clarke, Remote treatment of patients during the COVID-19 pandemic: digital technologies, smart telemedicine diagnosis systems, and virtual care[J], Am. J. Med. Res. 7 (2) (2020) 29–35

[6] Mashal, I., Alsaryrah, O., Chung, T.Y., Yang, C.Z., Kuo, W.H., Agrawal, D.P., 2015. Choices for interaction with things on Internet and underlying issues. Ad Hoc Networks 28, 68–90. [30] Mohanty, S.N., Ramya, K., Rani, S.S., Gupta, D., Shankar, K., Lakshmanaprabu, S., Khanna, A., 2020. An efficient lightweight integrated blockchain (elib) model for iot security and privacy. Future Generation Computer Systems 102, 1027–1037.

[7] Said, O., Masud, M., 2013. Towards internet of things: Survey and future vision. International Journal of Computer Networks 5, 1–17.: 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, pp. 230–234

[8] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., Sikdar, B., 2019. A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access 7, 82721–82743.

[9] Choudhary, S., Kesswani, N., 2018. Detection and prevention of routing attacks in internet of things, in: 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pp. 1537–1540.

[10] Choudhary, S., Kesswani, N., 2019. A Survey: Intrusion Detection Techniques for Internet of Things. International Journal of Information Security and Privacy (IJISP) 13, 86–105.

11] Choudhary, S., Kesswani, N., 2019. Cluster-based intrusion detection method for internet of things, in: 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), pp. 1–8

[12] P. Kocher, J. Jaffe, B. Jun, Differential power analysis, in: Proceedings of 19th Annual International Cryptology Conference, CRYPTO'99, in: LNCS, vol. 1666, Santa Barbara, California, USA, 1999, pp. 388–397.

[13] A. Wood, J.A. Stankovic, Denial of service in sensor networks, IEEE Comput. 35 (10) (2002) 54–62. [19] Y. Hu, A. Perrig, D.B. Johnson, Pachet leashes: a defense against wormhole attacks in wireless networks, in: Proceedings of IEEE International Conference on Computer and Communications, INFOCOM'03, vol. 3, San Francisco, CA, USA, 2003, pp. 1976–1986.

[14] D. Vujiıciťc, D. Jagodiťc, S. Randiťc, Blockchain technology, bitcoin, and Ethereum: a brief overview, in: 2018 17th International Symposium Infoteh–Jahorina (Infoteh), IEEE, 2018, March, pp. 1–6.

[15] Ethereum blockchain. https://ethereum.org/en/developers/docs/smartcontracts. (Accessed 13 March 2022).