Received on (07-07-2022) Accepted on (27-02-2023)

Blockchain-Based Secure Smart Health IoT solution Using RBAC Architecture

Faten F. Abushmmala[1], Aiman AbuSamra[1]
1 Department of Electrical Engineering, Islamic University of Gaza, Gaza, Palestine.
https://doi.org/10.33976/JERT.10.2/2023/1

Abstract— The revolution of Internet technology, which led to connecting everything through the World Wide Web, the Internet of Things (IoT) emerged to serve this need. IoT technology connects different devices, hardware, and software together, which are created to provide services and facilitate human life. The most critical application is in the health sector, where data privacy, security, and accessibility are demanding and agonizing challenges. In this paper, we use a block chain (BC) model that enforces the Role-Based Access Control (RBAC) model to address privacy and security concerns as well as the limited nature of IoT devices. The paper's concept is to divide the network according to the assigned role, and authentication and data transfer are thoroughly discussed. The Architecture of the proposed system is shown and displayed in flowcharts, where each node has different permissions and privileges. In the experimental part, two scenarios are applied; one where the network (IoT devices) is connected through an MQTT broker as an intermediary, and the second with BC that controls the IoT, which uses proof of assignment as a consensus model. The data flow shows that with BC, the network is much more secure and holds the privacy and integrity of the data.

Index Terms— IoMT, IoT, Blockchain, Health, RBAC.

I INTRODUCTION

Internet of Things (IoT) [1] is the technology that defined connecting wide range of diverse hardware's and technologies hence the word things, through the internet. The hardware's and the technologies features depend on the manufactures and the purpose. The purpose of the use for each is defined as the IoT applications, such as industrial, agriculture, retail, financial services and medical care, smart cities, smart buildings, smart factories and smart cars and so on. The rapid evolution is still on progress for IOT. More than 10 billion IoT devices were deployed globally by 2021 [2], and this figure is only a starting point; by 2030, it is expected to exceed 25.4 billion. 152,00 IoT devices are expected to be connected per minute in the year 2025. The IOT importance came from the diverse nature of these devices and the technology where each can provide and accomplish a task according to the application in hand. Some are just sensors used to sense the out area and provide information and reading for other hardware and software applications. The other important feature about IoT is that most of these "things" or devices are constrained, with limited power and limited resources which make them in desperate need for centralized architecture to organize its affairs. These IoTs also can cause major privacy and security menace [3] due to its low resources, its ability to handle encryption and other security measures are heavily expensive and not applicable easily. IoT has many applications, Medical IoT in particular some call it healthcare IoT [4], which mean using IoT in the Medical Industry. Many IoT devices created to serve such application, to manage its need and settings such as sensors and apps for remote healthcare monitoring, and telemedicine consultation and delivery. Medical IoT begun to engage AI and machine learning technology in its work in an attempt to support improvements to traditional medical devices., Medical IOT is the case study discussed in this paper. Securing and managing medical data obtained via IOT device is a challenging task, many attempts accomplished to achieve this goal.

Blockchain [5], on the other hand, is a kind of database. This database is distributed and decentralized, which is one of its appealing factors, since centralization can cause great danger for many reasons, such as: Centralized databases depend highly on the proposed network; the fear of bottleneck effect, especially with too many parties involved; the fear of one point failure if this database experiences any kind of trouble; besides all that, other problems can be encountered. The block chain can solve all of these features along with providing other attractive and compelling advantages such as security, transparency, and instant traceability**.** Blockchain (BC) first known in 2008 by a person or group of people

Satoshi Nakamoto [8], the main idea of the BC is to act as public ledger of cryptocurrency bitcoin, based on previuse work of Stuart Haber, W. Scott Stornetta, and Dave Bayer [7]. Satoshi Nakamoto is still obscure character remains unidentified to date.

In this paper, an attempt to integrate the IoMT (Internet of Medical Things for Patient Healthcare IoT Solution) with the Blockchain technologies that integrate the RBAC access model to regulate the data flow and to capture and share its advantages.

The goal of decentralizing IoT devices is something achievable conditionally due to the nature of IoT devices with different technologies and different hardware manufacturers. The need for authentication mechanisms, data transactions, IoT device management, and implemented security measures are all critical issues to consider before attempting integrating block chain into IOT systems. The main objective of this paper is to establish a corporate block chain in Smart Health IoT without centralization, which IoT requires due to many disadvantages of centralization, such as single point of failure and others.

Figure1. Smart IoT Health solution.

The paper is organized as follows background, related work, our methodology, experiments and results and finally conclusion.

II BACKGORUND

A Blockchain Technology

A BC is a growing list of records, a sequence of blocks, these block are connected using cryptography. Each block contains a cryptographic hash of the previous block. In a simple word, the BC is ledger to pass information from point to point in an automated manner. A transaction is created and stored in a block which must be verified by other parties. Once it's verified and distributed, the process creates a unique signature history which can't be replicated easily. The chain of blocks is similar to a ledger, which is a record or book of previous transactions for a certain entity. Of course, it will keep growing and growing with time. There are four types of BC [10]: public, private, consortium, and hybrid. Each of which encamps certain characteristics, you can choose the one that is more suitable for application. The benefits of BC are as follows: [11] 1) Data Integrity: Due to the nature of the BC, any attempt to edit is nearly impossible. 2) Free from Censorship: BC technology is not restricted to any human state, not related to politics or anything that can alter its integrity, as human records are. 3) Verifiable: BC technology the verification process is so complicated that any verified block is unquestionably legitimate. 4) Distributed: no single point of failure, no centralization disadvantages. 5) Traceability: everything can be traced to its sources and to the validation with data that can't be altered, which makes it perfect for achieving such a purpose. 6) Data integrity and data traceability result in immutability. 7) Open: One of the major advantages of BC technology is that it is accessible to everyone. 8) Stability: Once data has been validated to the BC, it is impossible to remove data (blocks) or attempt to alert. 9) Security: BC technology is highly encrypted in the chain, making it tougher for any hacker to disturb the traditional setup of the chain. 10) Faster processing: Before the invention of the BC, the traditional banking organization took a lot of time in processing and initiating transactions. 11) No third-party interference – The crypto currencies that use BC technology are not controlled by any government or financial institution. 12) Secure transactions – The BC is in charge of maintaining a record of all transactions that cannot be altered or manipulated. 13) Instant transactions – Transactions with BC technology are completed in a matter of minutes.

B Internet of things

By means of low-cost computing [12], physical things can analysis and collect data without human interaction.

C IoT and Blockchain for Healthcare

IoT for e-healthcare suffers from several shortcomings. The BC can solve them. IoT systems relay heavily on the server-client model. The server accomplishes the process of authenticating and any data processing needed. Storage capacity is a major issue that must be carefully considered; most IoT systems recommend a third party for data storage. Requiring third parties and servers is not practical for small IoT networks. For large-scale IoT networks, it is also expensive to set up several communication links, maintain centralized clouds, and network all of the equipment. In addition to the expenditures, the architecture is vulnerable to a single point of failure due to its reliance on cloud servers. Additionally, IoT devices need to be resistant to physical and informational hacking. Although some existing methods secure IoT devices, they are complex and unsuitable for resource-constrained IoT devices with limited computation power. Finally, BC is a P2P network, which solves the single-point-of-failure problem.

D Access Control Model

Access control model discuss the limits and privileges of accessing a system [13]. There are different types of Access control Model most important one is Attribute-Based Access Control (ABAC) and Rule-Based Access Control (RBAC or RB-RBAC). Attribute-based access control (ABAC) is an authorization model that evaluates attributes, to assign privileges and permissions. Rule-Based Access Control (RBAC) access control is an authorization model that evaluates roles to assigned privileges and permissions.

In this paper the RBAC model is revisited in the IoT Health applications.

In this paper, a new architecture for managing and securing IoT devices is presented in the health domain in particular. This architecture is decentralized without the need for a third party for authentication or for data storage as Blockchain requires and divided to suit the roles of the entities in the IoT health solution. The main idea is to divide the network into nodes. Each node can manage and authenticate its members. Each of these nodes' permissions and privileges depend on their role in the health IoT solutions. The access control model used to accomplish this is called the Role-Based Access Control (RBAC) model, where the role is the division factor. This paper takes high consideration of IoT limitations by making each IoT rely on the rest of the members in the same node, which will loosen the burden on the IoT processers.

II Related Work

Several papers suggested using BC for managing and securing the Internet of things, for instance. Srivastava et al. [14] evaluate various potentially suitable cryptographic technologies to secure IoT systems under BC technology, such as the ARX encryption scheme, Ring Signatures, and Diffie-Hellman key exchange technique. Ray et al. [15] propose data-flow architecture for IoBHealth. This architecture goal is to provide easy access, storge and manage these data. Authors in [16] suggest the framework of a BC-based key management protocol minimize the need for a centralized key authority while retaining similar security compared to its centralized counterpart. Li et al. [17] propose a unified authentication scheme for IoT BC devices based on PUF. The PUF model is used to authenticate IoT devices. It solves the heterogeneity problems of IoT device authentication schemes. Finally, the results showed that the proposed scheme is practical and executable. The authors in [18] propose a generic framework for PKI in IoT infrastructure using BC that can provide the functions of a CA. The authors of [19] discuss open issues and future trends in BC in IoT. Lao et al. [20] propose G-PBFT (Geographic-PBFT), a new location-based and scalable consensus protocol designed for IoT-BC applications, which is a modification of the PBFT (Byzantine General) consensus model, and shows good experimental results. G-PBFT exploits the geographic information of fixed IoT devices to reach consensus, reducing overhead significantly. Zhang et al. [21] use the smart contract to implement the ABAC access control model on the BC and combine the IPFS file system to achieve a decentralized The system's feasibility was tested. Huh et al. [22] proposed a management system for IoT devices using BC technology and providing security in the process. Authors in [23] suggested an architectural model for BC that enables IoT devices, multiple agents with role definition for each agent, and discussed their work to minimize the number of nodes, but the security risk will increase. Kim et al. [24] introduce "farm-to-fork", a food traceability application integrating the BC and IoT devices swapping messages. The goal is to create a distributed ledger accessible to all participants in the supply chain. Many other papers acts more like a guideline or a survey in the Blockchain/IoT subject such as : Authors in [25] discuss Blockchain and IoT distinguishing characteristics, architectural layout, distinguishing elements of both technologies, futuristic solutions for various real-world problems, various communication methods, and so on. In every subject, both technologies have a lot of distinguishing characteristics, but they also have limitations, which provide a futuristic route for research. A variety of distinguishing characteristics of technologies, as well as their frameworks and applications, are addressed. As security is significant concern in any system, many challenges and obstacles to provide the required level of security. New futuristic approach can be formulated in the light of these issues. Alam in this paper [26] also discuss the Blockchain application in IoT, the challenges, opportunities and of course platforms, but it particularly discuss three main challenges which are: Scalability, Storage and Lack of Skills and showing their major impact on the successes and the failure of any suggest framework that deploy both technologies Reyna et al [27] discuss the In relationship of integrating Blockchain and IoT, also investigates challenges in applying Blockchain IoT applications, and surveys most relevant work with analyzing order to analyze the process of integration and how much improvement can be achieved. Mohammad et al in [28] demonstrates the advantages and the challenges of integrating IoT and Blockchain. With showing different architectures to ensure secure data transactions and provide high management throughput. Also they discuss some good recent studies on the subject with showing future directions.

Most of the literatures have a common flaw: some architectures fail to account for the limitations of IoT devices, while others impose too many layers, causing complications in data handling and transfer. Any other proposed work that includes different layers of encryption and third party existence causes computation and communication overhead. Some architectures suggest using central authority, which conflicts with the point of using Blockchain technology, since the Blockchain idea is to have a distributed ledger instead of a centralized database that can be exposed to a single point of failure blemish. Our paper overcomes the mentioned shortcoming. No third party is needed. Each node is only responsible for its own entities. Decentralization remains true with Blockchain technology, while taking into account the limitations of IoT devices and avoiding unnecessary communication or computation overhead. It will be much clearer with the parts of the methodology.

Table1. Related work comparison		
Paper	**Pros**	**cons**
[14]	• The proposed system solve many security and privacy threats	• The proposed encryption framework imposes high computation on the limited IoT devices. • The proposed framework still theoretically, not proven work
[15]	• The paper provides comprehensive overview of consensus algorithms and technologies used in block chain in the context of e-health.	• The proposed system needs the existence of a third party.
[17]	• Ability to stand for multiple types of attaches (replay attacks, man in the middle etc). • Provide unified authentication process.	• Still need CA (centralized authority). • Need Hardware modifications of the IoT device.
[18]	• The level of trust among the proposed system is distributed which lead to minimize computation time. • The limited Iot is excused from the process.	• The proposed system relies in third party involvement. • The discussed frame work embodies many layers.
[20]	• Suggest consensus model for Permissioned block chain that provide low latency in comparison of others. • Also archives High scalability	• Comparison between G-PBFT over traditional PBFT consensus model no other consensus models discussed. • Discussing IoT devices as nodes, the constrains of IoT devices, limitations and heterogeneity not mentioned.
[21]	• ABAC IoT management model discussed. • The proposed system takes into account the IoT device heterogeneity. • High scalability (multiple accesses).	• There will be a significant communication overhead. • The process of authentication and classifying each IoT device consume times.
[22]	• Propose IoT management system to provide security and easy management using BC. • Also take power consuming into consideration.	• The scalability issue is not discussed. • Using RSA public key cryptosystems which is sensitive to factoring attacks [25].
[23]	• Propose architectural guideline for BC • Enabled IoT devices they defined multiple agents with multiple roles through adjusting the owner, renting period and the price of the IoT devices	• The suggest architecture minimize the need of multiple nodes through several process, but in the same time the communication overhead will be significant. • The IoT device limitation is not considered. • The security risk will increase with rules and agents methodology.

III METHOLDODY

IoT is known for its limitations, considering each IoT device to be a node in Blockchain technology doesn't make sense. For this purpose, each node consists of different IoT devices connected to a patient if he/she is in his home or hospital. These IoT devices are connected to smart tables/touch screens or lab tops, which are responsible for managing these IoT devices. There will be three types of nodes: patient node, doctor/nurse node, and administration node. The access control model applied here will be RBAC.

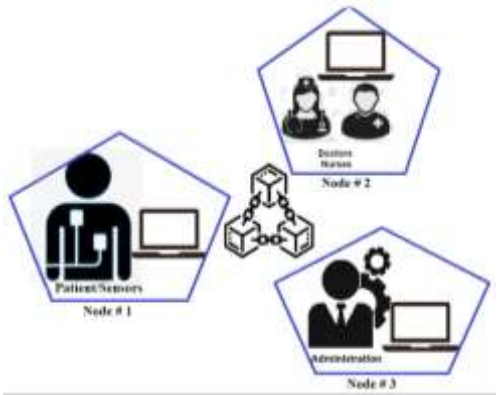

Figure 2. Blockchain IoT Health Solution.

The RBAC model is an access control that defines each entity, in our case, a node its privileges and permissions. The three types of nodes each have different types of responsibilities and privileges, and it makes no sense to give them equal access privileges.

The patient nodes should only supply the patients' data and reading. The doctor/nurse node can read and access data but cannot modify it and should be able to prescribe a line of medication and treatments. The last node, the administration node, can view both patient and doctor or nurse data but cannot alter this data. It can only manage and take statistics for management purposes. These nodes are confined to Blockchain Smart Contracts to organize their relationships.

The traditional Medical IoT was managed using an MQTT broker (Fig. 3). This type of network does not provide security and even defines roles in more limited ways.

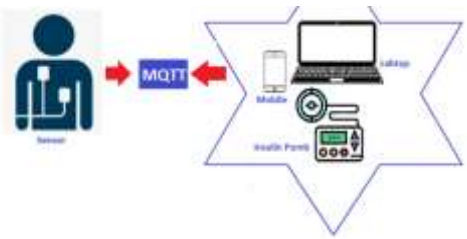

Figure3. Traditional Health IoT system.

MQTT broker works as intermediated which should transfer the data in secure and private way.

In our methodology, each node is responsible for authenticating their entities, which can be people or devices. All nodes are combined in block chain smart contracts under the RBAC access models, where each node is assigned a different role.

Every IoT device needs to go through a registration phase before being trustworthy and reliable. The authentication and registration phase are shown in **Fig.4.** After the authentication process is completed (which happens just once), the next phase is data transmission.

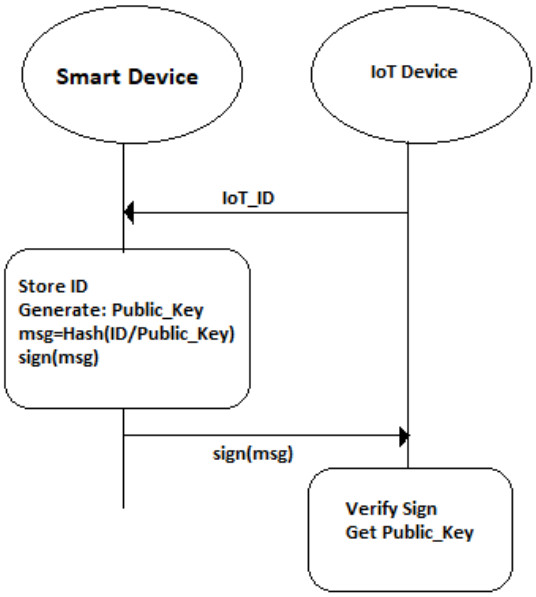

Figure.4. Patient Node Authentications process.

Every IoT device in the Patient Node will transmit the reading data, which will be collected and stored in the smart device, which could be a laptop, tablet, or even a Raspberry Pi.

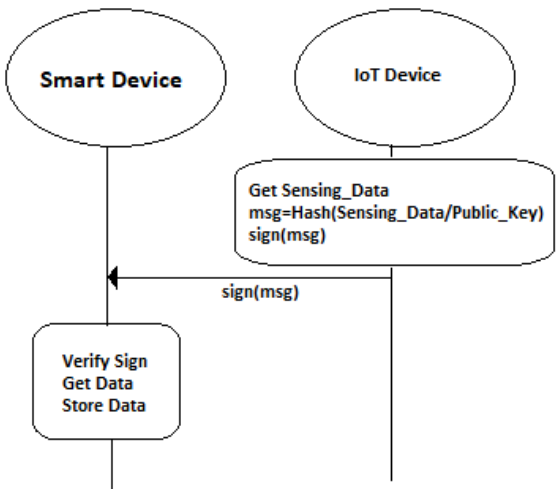

Figure.5. Getting Sensing Data in Patient Node for high capability IoT.

For other types of IoT devices that could be limited and cannot perform the process of registration and hashing, a direct connection will be established between the smart device and the lim-IoT. The smart device will be responsible for the process of verifying the lim-IoT device and processing the sensing data.

Second The Doctor/Nurse Node, every doctor/nurse must be validated through a unique ID **Fig.6;** after the process of validating, the public key generation and exchanging is executed.

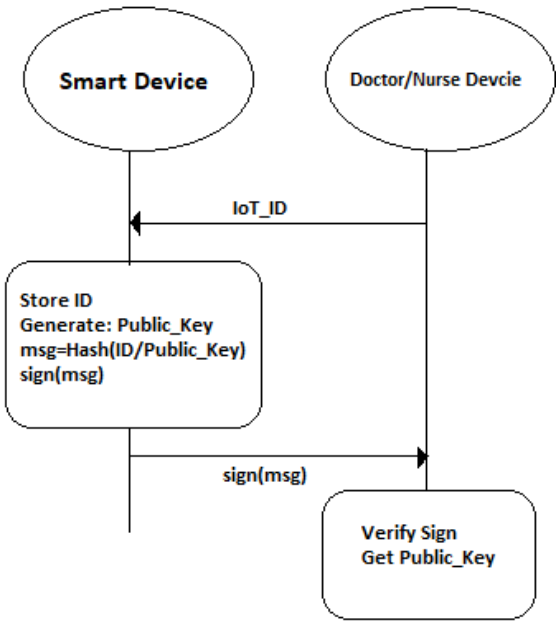

Figure.6. Doctor/Nurse Node Authentications process.

Finishing the authentication and registration processes came the process of exchanging the data. First the doctor or nurse requests to view the patient data. The request is verified and then the patient data is hashed using the public key and sent back to the doctor or nurse, who in return will process this data manually or automatically according to the nature of the data and create a treatment plan, which will be in the form of instructions.

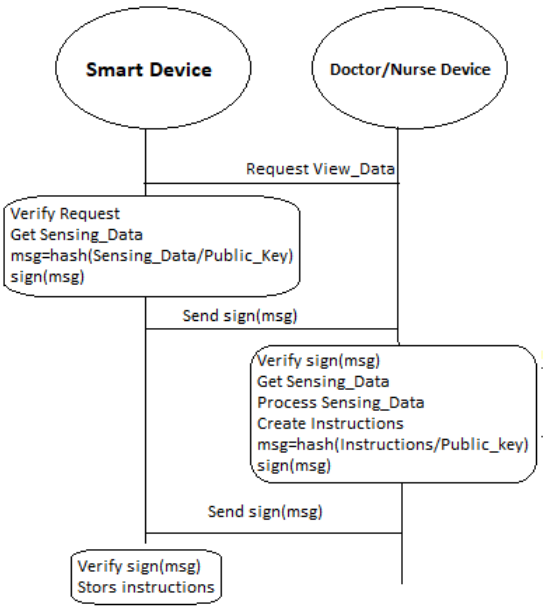

Figure.7. Getting Sensing Data in Doctor/Nurse Node.

Finally, the Administration Node, the process of authentication and registration is very similar to the Doctor/Nurse Node, but the process of getting data different according to the assign role. The Doctor/Nurse the only node that can provide treatment plan with instructions, but the Administration Node is role in managing which Patients Node must belong to which Doctor/Nurse Node, create statics in case request Shown in **Fig**.8.

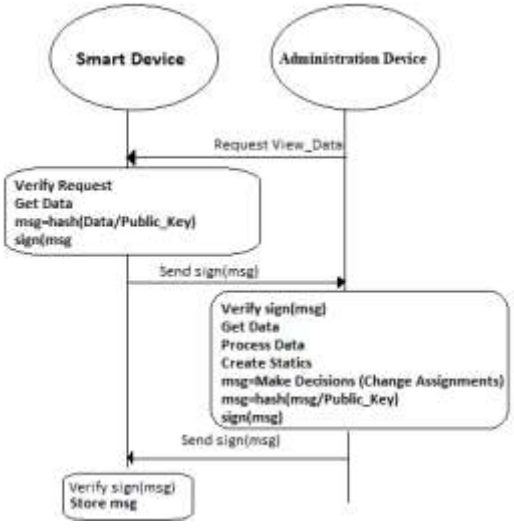

Figure.8. Administration Node.

The Administration Node has no authority to provide treatment plans or modify sensing data for a patient; it can only change assignment based on criteria such as doctor/nurse

specialty or geographical location.
The final process is the BC/RBAC model, each node will communicate through Blockchain and the Blockchain will enforce RBAC policy,

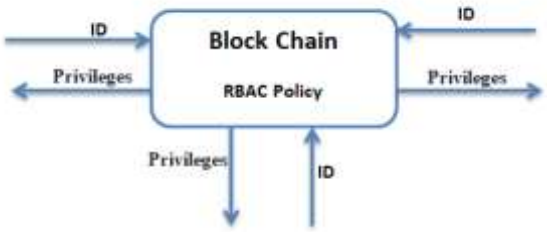

Figure.9. BC/RBAC Model.

First Node Identification and according the roles defined, after that the privileges become clear. The second phase **Fig**.10 shows the data exchange according each to their role.

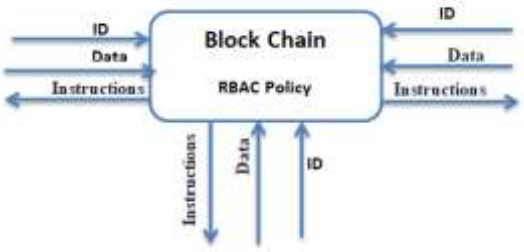

Figure.10. Data Exchange in the BC/RABC model.

Each node will send its data and receives Instructions that will force it to behave as requested **Fig.10** the number of nodes can vary and not restricted to three nodes, but there is various number of patient node, and various number of Doctor/Nurse Node and just one Administration Node.

IV RESULT AND EXPERIMENTAL

In this section the experimental results are discussed, Different IoT devices are connected through an Android App, Wire shark is used to verify the data privacy and security and compared it with another Android App that utilize the Blockchain in its work which called IOTW.

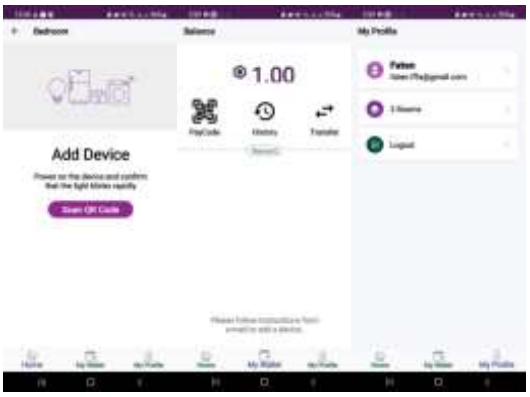

Figure.11. IOTW android App.

IOTW app see **Fig**.11, can be used to add as much as we need IoT and let it communicate with each other. This app facilities the management process of this IoT device.
IOTW platform uses device SDK. IOTW communication provides:

- Between mobile devices and IoT devices, there is a simple communication protocol.
- Different types of apps can be deployed quickly on IoT devices.
- Simple API for responding to events and messages from a mobile device application controlled by the user.

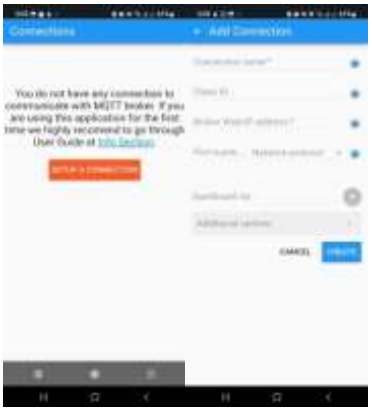

Figure.12**.** MQTT Android App.

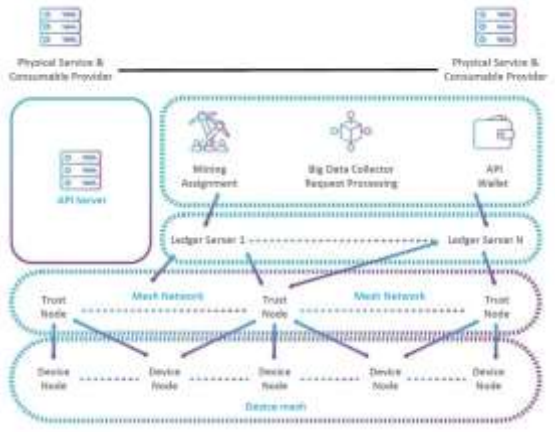

Figure 12. IoWT Flowchart

IoWT [29] create and integration of IoT and Blockchain using proof of assignment to accomplish the a decentralized network for the IoT applications with still achieving successful data exchanging. IoWT Fig.12 reduces system requirements on the IoT devices (end nodes) side; divide the Blockchain network into several levels. End nodes do not need to be computationally powerful or have a lot of memory. Without any hardware changes, every IoT device can connect to our Blockchain. The chances of receiving Blockchain awards are same for all end nodes. The chain consumes no superfluous energy, and it can handle instant transactions no matter how large it becomes.

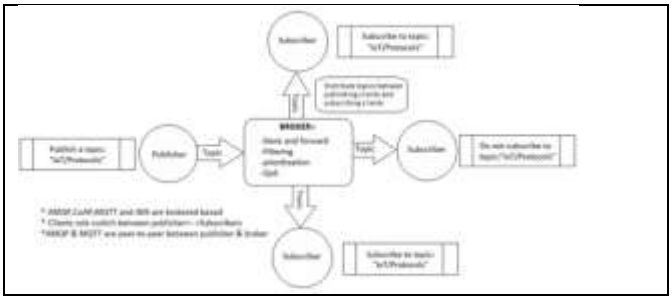

Figure 13. MQTT Protocol Flowchart.

MQTT consist of MQTT broker and MQTT clients shown in **Fig**.13 , the broker job is to distribute the messages among IoT's devices. Every MQTT message consists of topic, the client publishes a message related to a topic, and each MQTT clients subscribe to the topics that want to communicate with. The MQTT broker uses the topic with its list of subscribers to manage the messages and send it to the suitable clients. In case of connection get broken, the messages buffered by the broker, and sent back in case of the connection are activated. in case of publishing client cannot connected to the broker, the broker will close the connection send subscribers the messages cached with instructions included from the publisher.

In the results the First where IoWT is used, the messages sent and received will be hashed, but in the case of MQTT broker/client scenario the topic can be easily seen by wirhsark and figure these topics out which is considered a serious data leak.

V CONCLUSION

Different papers deploy the use of Blockchain in IoT solutions. In this paper, we are more concerned with health IoT solutions. This paper proposes the use of an orthodox access control model called Role-Based Access Control (RBAC), which assigns privileges and permissions according to the entity role. IoT devices came from different manufacturers with different technologies, and their capabilities for processing and handling data differed. Some IoT devices came with no processing capability at all.

In this paper, a network of nodes is constructed where each node consists of different devices, some of which are limited while others are not. These devices will help each other to perform much better. The blockchain will enforce the RBAC model to organize the data flow among these nodes. In each node, there is a process of authentication and registration that comes before the data exchange process to ensure privacy. A practical use case is deployed using two known Android apps used for managing IoT devices; one that deploys the MQTT protocol and the other uses Blockchain technology. A comparison between the two apps' data flow privacy is executed, and the IOTW app (Android app uses BC) performs much safer. The data privacy and integrity are still held. Futuer work would be applying hardware experimental and viewing the data security, privacy and scalability in case of multiple IoT devices.

REFERENCES

[1] D. Minoli, K. Sohraby and B. Occhiogrosso, "IoT Considerations, Requirements, and Architectures for Smart Buildings—Energy Optimization and Next-Generation Building Management Systems," in IEEE Internet of Things Journal, vol. 4, no. 1, pp. 269-283, Feb. 2017, doi: 10.1109/JIOT.2017.2647881.

[2] "Internet of Things (IoT) - statistics & facts",Technology &Telecommunications› Consumer Electronics, Published by Lionel Sujay Vailshery, May 11, 2021.

[3] Habtamu Abie, Silvio Ranise, Luca Verderame, Enrico Cambiaso, Rita Ugarelli, Gabriele Giunta, Isabel Praça, Federica Battisti ,"Cyber-Physical Security for Critical Infrastructures Protection" First International Workshop, CPS4CIP 2020, Guildford, UK, September 18, 2020, Revised Selected Papers,Springer Nature, Feb 17, 2021.

[4] Chakraborty, Chinmay, "Smart Medical Data Sensing and IoT Systems Design in Healthcare", IGI Global, Sep 20, 2019.

[5] S. E. Chang and Y. Chen, "When Blockchain Meets Supply Chain: A Systematic Literature Review on Current Development and Potential Applications," in IEEE Access, vol. 8, pp. 62478-62494, 2020, doi: 10.1109/ACCESS.2020.2983601.

[6] Nakamoto, Satoshi (October 2008). "Bitcoin: A Peer-to-Peer Electronic Cash System" (PDF). bitcoin.org. Archived (PDF) from the original on 20 March 2014. Retrieved 28 April 2014.

[7] Bayer, Dave; Haber, Stuart; Stornetta, W. Scott (March 1992). Improving the Efficiency and Reliability of

Digital Time-Stamping. Sequences. Vol. 2. pp. 329–334. CiteSeerX 10.1.1.71.4891. doi:10.1007/978-1-4613-9323-8_24. ISBN 978-1-4613-9325-2.

[8] Rodbard, D.: Continuous Glucose Monitoring: A Review of Successes, Challenges, and Opportunities. Diabetes Technology & Therapeutics, S2-3–S2-13. (2016)

[9] . Gia, T., Ali, M., Dhaou, I., Rahmani, A., Westerlund, T., Liljeberg, P., Tenhunen, H.: IoT-based continuous glucose monitoring system: A feasibility.

[10] Harvard Business Review, Don Tapscott, Marco Iansiti, Karim R. Lakhani,"Blockchain: The Insights You Need from Harvard Business Review", ,Publisher Harvard Business Review Press, 2019, ISBN 1633697916, 9781633697911

[11] Saifedean Ammous,"The Bitcoin Standard: The Decentralized Alternative to Central Banking",Publisher John Wiley & Sons, 2018, ISBN 1119473861, 9781119473862

[12] Samuel Greengard,"The Internet of Things",MIT Press, Mar 20, 2015 - Technology & Engineering.

[13] "NFC access control: cool and coming, but not close". Security Systems News. 25 September 2013. Archived from the original on 6 April 2014. Retrieved 30 March 2014.

[14] Gautam Srivastava, Jorge Crichignoz, and Shalini Dharx, "A Light and Secure Healthcare Blockchain for IoT Medical Devices", 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), 978-1-7281-0319-8/19/$31.00 ©2019 IEEE

[15] Partha Pratim Ray ,Dinesh Dash, Member, Khaled Salah and Neeraj Kumar , Senior Member,"Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases",1937-9234 © 2020 IEEE,Digital Object Identifier 10.1109/JSYST.2020.2963840

[16] Kanwalinderjit Gagneja, Riley Kiefer, "Security Protocol for Internet of Things (IoT): Blockchain-based Implementation and Analysis", April 14,2022 at 21:46:21 UTC from IEEE Xplore

[17] Dawei Li, Yingxian Song, Lixin Zhang, Di Liu, Baoquan Ma, Zhenyu Guan," Unified Authentication Scheme for IoT Blockchain Based on PUF",2021 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)]

[18] Deepa Pavithran, Khaled Shaalan, "Towards Creating Public Key Authentication for IoT Blockchain",978-1-7281-5061-1/19/$31.00 ©2019 IEEE

[19] Avelino F. Zorzo, Henry C. Nunes∗, Roben C. Lunardi, Regio A. Michelin and Salil S. Kanhere, "Dependable IoT using blockchain-based technology",978-1-5386-8489-4/18/$31.00 ©2018 IEEE, DOI 10.1109/LADC.2018.00010

[20] Laphou Lao, Xiaohai Dai, Bin Xiao∗ and Songtao Guo, "G-PBFT: A Location-based and Scalable Consensus Protocol for IoT-Blockchain Applications",1530-2075/20/$31.00 ©2020 IEEE DOI 10.1109/IPDPS47924.2020.00074

[21] X. Zhang and X. Jiang, "IoT Architecture Based on ABAC Smart Contract," 2020 3rd International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE), 2020, pp. 122-128, doi: 10.1109/AEMCSE50948.2020.00033

[22] S. Huh, S. Cho and S. Kim, "Managing IoT devices using blockchain platform," 2017 19th International Conference on Advanced Communication Technology (ICACT), 2017, pp. 464-467, doi: 10.23919/ICACT.2017.7890132

[23] M. Shurman, A. A. -R. Obeidat and S. A. -D. Al-Shurman, "Blockchain and Smart Contract for IoT," 2020 11th International Conference on Information and Communication Systems (ICICS), 2020, pp. 361-366, doi: 10.1109/ICICS49469.2020.239551

[24] M. Kim, B. Hilton, Z. Burks and J. Reyes, "Integrating Blockchain, Smart Contract-Tokens, and IoT to Design a Food Traceability Solution," 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2018, pp. 335-340, doi: 10.1109/IEMCON.2018.8615007.

[25] Vikash Kumar Aggarwal, Nikhil Sharma, Ila Kaushik, Bharat Bhushan, Himanshu, "Integration of Blockchain and IoT (B-IoT): Architecture, Solutions, & Future Research Direction",Vikash Kumar Aggarwal et al 2021 IOP Conf. Ser.: Mater. Sci. Eng. 1022 012103.

[26] Tanweer Alam , "Blockchain and its Role in the Internet of Things (IoT)",International Journal of Scientific Research in Computer Science, Engineering and Information Technology 2019 IJSRCSEIT |Volume 5|Issue 1|ISSN : 2456-3307, DOI: doi.org/10.32628/CSEIT195137.

[27] Ana Reyna∗, Cristian Mart´ın, Jaime Chen, Enrique Soler, Manuel D´ıaz, "On blockchain and its integration with IoT. Challenges and opportunities", 2018.

[28] Arshiya S Mohammad, M Nawaz Brohi , Iftikhar Alam Khan, "Integration of IoT and Blockchain", Technium Vol. 3, Issue 8 pp.32-41 (2021) ISSN: 2668-778X www.techniumscience.com

[29] Fred Leung, Tony Chan, Ka rtik Mehrotra, and Peter Chan," A Scalable Blockchain – Proof of Assignment Protocol",2020,Whitepaper