A DECENTRALISED AUTHENTICATION AND ACCESS CONTROL MECHANISM FOR MEDICAL WEARABLE SENSORS DATA

1st Mwrwan Abubakar
School of Computing
Edinburgh Napier University.
Edinburgh, UK
m.abubakar@napier.ac.uk

2nd Zakwan Jaroucheh
School of Computing
Edinburgh Napier University.
Edinburgh, UK
z.jaroucheh@napier.ac.uk

3rd Ahmed Al Dubai
School of Computing
Edinburgh Napier University.
Edinburgh, UK
a.al-dubai@napier.ac.uk

4th Bill Buchanan
School of Computing
Edinburgh Napier University.
Edinburgh, UK
b.buchanan@napier.ac.uk

***Abstract*—Recent years have seen an increase in medical big data, which can be attributed to a paradigm shift experienced in medical data sharing induced by the growth of medical technology and the Internet of Things. The evidence of this potential has been proved during the recent covid-19 pandemic, which was characterised by the use of medical wearable devices to help with the medical data exchange between the healthcare providers and patients in a bid to contain the pandemic. However, the use of these technologies has also raised questions and concerns about security and privacy risks. To assist in resolving this issue, this paper proposes a blockchain-based access control framework for managing access to users' medical data. This is facilitated by using a smart contract on the blockchain, which allows for delegated access control and secure user authentication. This solution leverages blockchain technology's inherent autonomy and immutability to solve the existing access control challenges. We have presented the solution in the form of a medical wearable sensor prototype and a mobile app that uses the Ethereum blockchain in a real data sharing control scenario. Based on the empirical results, the proposed solution has proven effective. It has the potential to facilitate reliable data exchange while also protecting sensitive health information against potential threats. When subjected to security analysis and evaluation, the system exhibits performance improvements in data privacy levels, high security and lightweight access control design compared to the current centralised access control models.**

***Keywords*—Internet-of-Things, Medical wearable devices, Blockchain, Access control.**

I. Introduction

There have been reports of a dramatic rise in the number of medical patients across different parts of the globe, making it difficult for patients to access healthcare services. However, the healthcare industry has experienced significant growth and changes in E-health applications, which has been attributed to the rise of innovative technologies such as the Internet of Healthcare Things (IoHT) and mobile cloud computing [1]. The rise of the Internet of Things and wearable technology has brought opportunities to help solve such challenges in the healthcare domain. Such technology is facilitated by big data analytics and cloud computing, which collect data from numerous individual devices and pool them into big health data that can be used to derive valuable insights. This data can be used by hospitals and medical institutions to link to other Electronic Health Record (EHR) Data in a bid to facilitate disease diagnoses, disease treatment, and health monitoring. This data can also be useful to insurance companies in coming up with strategic and detailed policies guided by individual characteristics, which will be more beneficial to customers since they will get to choose insurance plans that fit their medical needs [2]. The availability of wearable sensors and mobile devices have enabled patients to handle their health data at home and share it with a healthcare provider, facilitating timely medical access and support from healthcare personnel. With the Internet of Health Things in place, healthcare providers can monitor their patients and offer them care remotely, which helps in healthcare delivery and is also economically beneficial to patients. The Internet of Health Things also allows the tracking of patient health by healthcare providers, who can, in turn, advise the patients and offer them the required medical services. However, there are cases where patients will be unable to track and manage their health records shared with the healthcare provider or even find it default to do so.

A. Problem statement

A secure data sharing infrastructure is needed to handle the sharing of health data between institutions. However, this is marred by several changes regarding interoperability, security, and privacy. Health data is categorised as highly privacy-sensitive, and storing it in a public cloud increases the risk of unauthorised access and exposure. The current use of a centralised architecture in healthcare requires a centralised trust for it to function properly. There is also the challenging task of effective health data integration and healthcare systems operability, in addition to users having little to no say regarding data collected on their health. To help achieve self-sovereignty and increase the adoption of wearable devices and mobile platforms, there is a need for improved versions of IoHT systems that protect user privacy and provide user-centric access control. Operating on a central authority has its own share of risks, such as single point failure, which is often solved by using third parties to provide data backups, effectively

increasing the risk of exposure [3]. This necessitates the need to develop efficient access control solutions for medical data sharing. On the other hand, there is considerable potential for blockchain and decentralised technologies, which exclude the use of a third party to manage the trust. Decentralisation of trust is increasingly becoming a dominant trend, creating opportunities to manage authentication and authorisation in a decentralised and autonomous manner. Therefore, blockchain technology can revolutionise healthcare applications by providing promising solutions that promote healthcare security and performance. Through this research, we have worked on designing a secure access control framework for medical wearable devices. The remainder of this paper is organised as follows. Section 2 discussed the related work and our contribution. Section 3 provided background on blockchain technology. In section 4, we present our proposed solution. Section 5 looks at the system design. The system entities are presented in section 6. Section 7 looks at the system interaction and information exchange. In section 8, we described the implementation of our solution. We provided performance and security analysis of our proposed mechanism in section 9. Finally, we conclude our paper in section 10.

II. Related work and Our Contribution

The global Electronic Health Records (EHR) market is predicted to expand from around 30 billion in the year 2020 to 40 billion by 2025. However, the security of the EHR remains a major challenge in managing EHR data [4]. A significant of current researches are focused on security and privacy in the IoHT. For instance, the literature in [5] [6] [7] analysed the side-channel attacks that may be influenced by devices such as wearable medical devices and smartwatches. Similarly, the authors in [8] [9] discussed the security issues of key negotiation, data encryption and integrity during transmission. There have been several efforts [10] [11] [12] to address these security issues by proposing access control mechanisms for IoHT. However, the issue with these solutions is that they are centralised. The authentication data needs to be stored in a centralised local server, prone to a single point of failure. In addition, when encryption is used for authentication, some complex encryption algorithms will also bring some problems, such as low computational efficiency, increasing hardware power consumption, etc. Lately, several research efforts were geared towards finding solutions to the key challenges of access control on IoHT by proposing integrating blockchain technology with IoHT to meet the IoHT security needs. For instance, the work presented in [13] investigated the blockchain applicability to overcome various security issues in IoT and proposed a blockchain-based authentication mechanism. The main issue with the proposed approach is that one system's devices cannot interact with the devices in other systems. Hence, it is not suitable for many distributed IoT applications that require interaction with devices in different systems. Another approach was highlighted in [14], which proposes a hybrid architecture that provides decentralised access control to the e-heath data by utilising both blockchain and edge nodes. The proposed architecture uses blockchain to manage users' identities and access control policies. The e-health data is stored on the off-chain edge nodes and implement policies defined in Abbreviated Language For Authorisation (ALFA) to apply attribute-based access control that relies on the blockchain-based access control logs. The proposed system was implemented using Hyperledger Fabric blockchain. Similarly, the authors in [15] proposed an approach to allow patients to grant access to their health information stored on a blockchain to assigned individuals. In the previously proposed blockchain-based approaches, the users' health information is stored on the blockchain. However, the blockchain has been questioned regarding its ability to securely store data, as the completed transparency is contrary to confidentiality. Besides, the principal characteristic of the blockchain is preserving the integrity of data by rendering it immutable. Nevertheless, this feature may be a double-edged sword. The reason is that errors shared over the distributed ledger cannot be corrected or, in the case of users need to delete their personal health data. In addition, solving the privacy issue by placing the entire health records into a private blockchain would considerably enlarge the entire chain size, demanding more storage at each node.

A. Our Contribution

Our main contributions in this paper can be summarised as follows.

- Blockchain-based authentication and authorisation mechanism for medical wearable devices.
- A decentralised access control and data access delegation approach for sensitive medical data propagated from the users' health wearable devices.
- A proof-of-concept implementation of the proposed solution along with performance evaluation and security analysis, which obviously proves the viability of our system to satisfy the IoT security requirements.

III. Background on Blockchain

Blockchain technology was initially proposed by Satoshi Nakamoto [16] to provide secure financial transactions. It is a distributed database, which meets the features of asymmetric encryption, tamper resistance, and decentralisation. Blockchain is made up of blocks related to each other through a chain, with each block consisting of transactions, transaction counter, and block header. The first block in the blockchain system is known as 'Genesis'. Blockchain offers a decentralised architecture that can be used to record data. The consensus mechanism offered by a blockchain is one of the most significant and fundamental blockchain technology inventions. Security in the blockchain is implemented through a proof of work concept, whereby a transaction is only deemed valid once the system obtains the proof. The proof lets the system know that enough computational work was exerted on the transactions by the authorised nodes [17]. This process, which leads to the creation and addition of new blocks, is known as mining. Every block in a blockchain has a hash in its header, generated by the Secure Hash Algorithm (SHA-256)

and used for identification purposes. A block's header also contains the address of the previous block in the blockchain. The Secure Hash Algorithm calculates a fixed size 256-bit cryptographic hash from any size plain text.

A. Blockchain and e-health

The advanced blockchain technology developments were first applied in cryptocurrencies such as Ethereum [18] and Bitcoin [16]. While blockchain technology remains significant in cryptocurrencies, it can also be used on any application requiring secure authentication, such as IoHT. This is because blockchain technology comes with a secure cryptographic technique, which can be used to identify and authenticate systems and users, thus facilitating access control in a secure, distributed, and scalable manner. Using blockchain in such a system is critical for data control. E-health can rely on new security features of the blockchain-based access control, which are more advantageous compared to traditional access control solutions. One such advantage is creating immutable ledgers containing transactions to be used in a data-sharing system, thereby guaranteeing high system integrity and trustworthiness. Therefore, once a transaction has been recorded, it cannot be altered or modified by anyone since blockchain only records transactions and does not permit recovery actions to its records [2]. Blockchain-based smart contracts have also proved critical in user verification and authentication [19]. The strict access control policies in smart contracts are essential in the authorisation of users and in detecting and preventing potential threats to IoHT systems. Finally, the use of smart contract technology with blockchain eliminates the need for a central server, therefore maintaining fairness among transacting parties. Since all the smart contracts in the blockchain are public, all connected users will have a copy of the smart contracts, getting equal rights to exercise control over contract operations [19].

IV. The proposed solution

This study aims to adopt blockchain technology to design a secure framework for medical wearable devices. To solve privacy and security challenges in IoHT systems, we propose a blockchain-based decentralised identity system and privacy-preserving data access control method to facilitate data sharing with the authorised people. This will ensure that users have full control over their personal data instead of having it stored and managed by a third party. The system's architecture will adopt a public blockchain structure. The proposed solution exhibits the effectiveness of a blockchain-based access control mechanism, which allows for delegated access permissions facilitated through a distributed ledger for information, services, and any devices within the Internet of Health Things systems. To achieve secure data sharing, users will have access permissions managed via a smart contract. This means that the resource owner can set access rules and eliminate the need for a third party to manage the data and determine who can access the data. To ensure users' health information security and privacy, it will be stored on a database hosted on a trusted platform rather than on the blockchain. The use of blockchain technology in this system remains for delegated access control and secure user authentication. The proposed solution can be applied to various IoT applications since it is suited to meet specific IoT requirements regarding defence against attacks, lightweight, distributed nature, and scalability while also meeting the CIA (Confidentiality, Integrity, and Availability) security triad requirements.

V. System Design

The proposed blockchain-based IoT platform will comprise four layers: the users' application layer, healthcare IoT sensors layer, connectivity layer, and the blockchain service layer.

A. Users' application layer

The application layer will provide a user interface for presenting data collected from wearable devices into the users' application interface. Wearable devices, such as body temperature sensors and ECG, will collect health data from the users and then upload them to a secure database hosted by our application. Once the data is recorded, the users will remain the sole owner of their health data. Additionally, this layer allows users and resource owners to manage their accounts and set users policies by communicating with the smart contracts on the blockchain. Only the owner can grant, revoke or deny access to data to third parties such as medical personnel. The users can grant the health providers access to their data when seeking medical treatment or record data relating to a certain treatment to help the professional monitor their health and improve or adjust treatment.

B. Healthcare IoT sensors layer

This layer is made up of different medical wearable devices that are capable of communicating, storing data, and computing. Wearable devices help transform original health data into an understandable format and sync it to an online account. A user account can have either a single wearable device or multiple wearable medical devices.

C. The connectivity layer

The connectivity layer offers routing management and is responsible for network management, message brokers and security management, etc. The communication is made through the Message Queuing Telemetry Transport (MQTT) protocol [20] which allows the transmission of sensors data from the wearable device to the users' application layer. MQTT is a publish/subscribe protocol where the broker has to push information to the client, as opposed to the request/response model that is currently used in the HTTP protocol, which requires a client to request data. Once the medical sensors layer collects raw data, it is sent to a master MQTT broker, which it works as a messaging broker to aggregate and distributes the data to the resource owner or any other individual granted access by the data owner [20].

D. The blockchain layer

We use Ethereum-based blockchain on the proposed model to help store information in a distributed manner. The reason for using an Ethereum-based blockchain is because it allows the deployment of smart contracts in their blockchain system. Smart contracts will be responsible for any authentication and authorisation processes. Since using smart contracts would make interfacing data stored on the blockchain possible, we developed them in such a way that they register the client's remote devices and can set the user policies. The smart contracts used in the system will also store a trusted mapping between a public key authorised by the user and its access token. The client's identity will have the public part of the asymmetric key pair and will be able to verify that the user accessing the blockchain is using an authentic message signed by the key pair's owner.

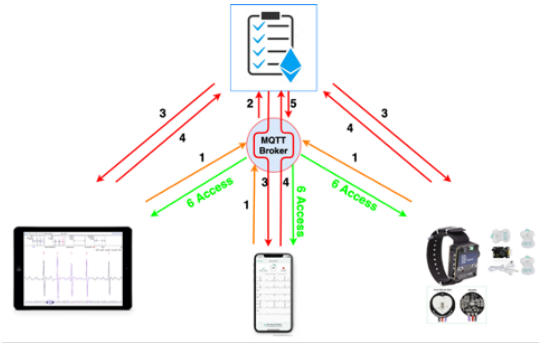

Fig. 1. **The proposed system design.**

(1) Send connect request to the broker. (2) The broker sends the user ID to the smart contract for authentication. (3) Smart contract generates a random value (challenge) (4) the users receive the random value and sign transaction using the user's private key to be sent to the smart contract. (5) The smart contract sends back the result of the process to the broker (6) The broker will then grant the user access and connect the users.

VI. System Entities

The proposed system is comprised of a number of entities such as clients, an MQTT messaging server, and a smart contract. The clients include health wearable devices, healthcare providers, and resource owners.

A. Resource owner

The system's resource owners are the Ethereum clients, who have both a public and private key. Users issue transactions signed by their private key, whose hash is taken to be the user's address and associated with their access token. Before using the system, the users will be required to set user policies, assign users to specific topics and register their remote devices. After registration, the users will be able to control access to their health data. This will be achieved through the mobile app, which can share and communicate user data securely to the smart contract. Our approach does not require the data to pass through a central authority as users can use their device storage to store their credentials.

B. MQTT messaging server

The MQTT broker is responsible for providing sensor readings and processing user requests. The broker is similar to other users in the system since they are all on the Ethereum blockchain and have both private and public keys. Anytime a connect request is sent by a client, the MQTT broker will extract the public part of the key pair, which is the client's ID. This information will then be sent to the smart contract for verification. Once access is allowed, the smart contract generates a challenge to serve as a one-time password for authenticating clients. The clients, in turn, sign the challenge with their private key. The MQTT broker will then validate the procedure's correctness and grant or deny access. The MQTT broker can either run on a specific host or reside on the cloud.

C. Smart contract

The proposed model exploits the advantages of smart contracts and blockchain technologies in performing delegated authorisation in IoT systems. Smart contracts help to store an immutable record of both user policies and authorisation information. They also offer resilience by executing smart contract code across all blockchain nodes. The smart contract will be used to implement policies such as on-chain access control decisions. The smart contracts will help with issuing tokens used by both publishers and subscribers to authenticate to the MQTT broker. Using smart contracts ensures that users do not have to store their tokens locally as it helps generate access tokens and manage their authentication process. The integrity and authenticity of the access token, which serves as an OTP (one-time-password), can be verified by a simple lookup in the distributed ledger. The web3 JS library, which uses the RPC to interact with the smart contract, will be used to access all the services written in the smart contract.

D. Healthcare providers

The user will appoint the healthcare providers, such as doctors, to provide medical treatment or suggestions. The system will allow the healthcare provider to upload the user's medical treatment data to the medical health record for the purpose of sharing it with other medical professionals but only after obtaining the patient's permission. The health provider can also request access to the user's health data from a wearable device or medical treatment data from the record through the proposed system. The smart contracts help grant access to every data request and access on the blockchain by implementing policies.

VII. Systems Interactions and Information Exchange

Interactions between the entities in the system are also known as transactions and have to be validated before they can be confirmed. The interaction occurs in two phases, which include:

A. The registration phase

For the registration, the user starts by downloading a mobile app on their smartphone phone. The user needs to create an Ethereum account and get private and public keys. The private key will be used to sign transactions from the user's account and will be stored on the user's device. The users' public keys will be associated with their identities. For the user to send the required information (topic name, user's role, and the remote device ID), needs to submit transactions to the smart contract. The mobile app will then rely on the functionalities of smart contracts to set policies and add the IoT devices to the user's list of trusted devices.

B. The Authentication phase

Anytime a client uses the client mobile app to request access to the broker, the application will start the authentication process by sending a connect request to the broker and pass the client ID. Besides, the broker verifies the users' permissions by sending the user's ID to the smart contract to verify the user's permissions. Once the request is permitted, the smart contract will generate a challenge, which will require the user to sign it using the private key. The user will then get a notification on the app to either approve or deny the signing request. Once the broker retrieves the verification result from the contract, an authorised connection with the client is created.

VIII. Implementation

This section explains the technologies used and the implementation process of our system. The study used a case study involving a patient who is being remotely monitored by a doctor through medical devices such as body temperature and ECG sensors. The prototype is made up of four components, including the messaging communication system, the wearable medical devices, a smart contract to help interface data on the blockchain, and the client application.

A. The blockchain implementation environment

We implemented the Ethereum blockchain smart contracts as a proof of concept. The choice of Ethereum blockchain is based on its ability to deploy smart contracts and the support that comes with its popularity. To implement our smart contracts, we used Solidity, a Turing complete language that helps develop smart contracts in the Ethereum blockchain systems. We then used the Ethereum-based IDE Remix to write, evaluate, and deploy smart contracts across the Ethereum network. The IDE also comes with a compiler that can be used to test the functionality of smart contracts.

B. The communication protocol

The MQTT protocol will be the main communication protocol used to facilitate data transfer from the IoT devices to the user application. We utilised the open-source Mosca MQTT broker [21] to help with the implementation of the MQTT server as it helps with data exchange between subscribers and publishers or between a mobile application and a wearable medical device. To help bridge the blockchain framework to the MQTT application for the authorisation and authentication of clients, we used a JavaScript API.

C. The users' client app

We will use a web socket to establish communication between the user's mobile app to the MQTT broker and facilitate real-time data exchange. Our application will help manage the user interface, managing user profiles, and communicate with the smart contracts on the blockchain. We build a native mobile app using JavaScrip. To make communication between the Ethereum blockchain and our application possible, the proposed system uses a web3.js Ethereum JavaScript API that interacts with an Ethereum node run on Infura.

D. The wearable device

To build the medical wearable device, we utilised an ESP32 DevkitC v4 board. We also added an AD8232 ECG sensor to help with ECG monitoring. We then used the Zerynhth studio, which offered a platform we could use to program microcontrollers using C and Python programming languages and offers an open-source Python library that can interact with smart contracts and the Ethereum blockchain. The Zerynth Ethereum library uses the JSON-RPC interface to send transactions and interact with Ethereum nodes. This makes it possible to make transactions and fetch status information. This library offers access to two companion classes that help with building a higher-level interface, and they include transaction and contract. The contract class can help call smart contracts and their methods, while the transaction classes help develop a correctly signed transaction that is ready to be sent.

IX. Evaluation

A. Security analysis

This section will highlight how our proposed system will resist the potential security threats for an IoT system. Medical data sharing systems face great security concerns regarding the protection of sensitive patient information from potential security threats and attacks. We will start by evaluating the security margin of our model when faced with different threats.

1) Man in the Middle attack (MITM: The proposed model will utilise the cryptographic signature and random challenges to help prevent potential MITM attacks. The system will remain safe from such attacks since the smart contracts produce only one unique challenge, which can be mapped to a single user. Additionally, the model will also require users to use their private key when signing the challenge to access the system.

2) Sybil Attack: To help protect the model from a Sybil attack, each device will be assigned a unique identifier stored on the blockchain. Each entity connected to the model will have a single key pair at any particular time. The private key will only be known by its user while the public key remains visible to all entities signed into the blockchain network. This means that the adversary cannot access a private key, which is used to sign the transaction for data access. Without the private key, adversaries cannot forge a user's signature. Additionally, all invalidated transactions are removed from the blockchain network, making our system resistant to external attacks.

3) Denial of service (DOS) Attack: During a DoS attack, the attacker makes it difficult for an authentic user to access the service in the network by increasing traffic or launching fraudulent transactions. However, due to the decentralised nature of blockchain, our model becomes resistant to DoS and DDoS-related attacks. The large number of mining nodes in Ethereum makes it highly resistant to DDoS attacks. Therefore, our model ensures high data availability for authentication data that is saved on the Blockchain. Even if a node fails or becomes unreachable, the network as a whole will continue to operate. As a result, our system will continue to operate at a high level of availability.

B. Security of our system

Every model comes with three main security requirements that model designers need to address, and they include confidentiality, integrity and availability. In this section, we analysed the security of our system based on these requirements:

1) Tamper-proof: The system does not allow the modification of the users' policies, access rolls or credentials as they remain immutable. Due to the chronologically nested blocks, which contain a hash of the previous block and the current timestamp, transactions remain immutable unless one individual takes over 51% of the network's computational power. The blockchain records every access request and access activity, meaning that any changes made to the data can be audited and tracked. Additionally, each transaction has a digital signature that provides the non-repudiation, integrity, and authentication of each transaction.

2) Privacy preservation: The users' credentials remain highly sensitive and should not be disclosed to any third party without approval from the patient. To tackle the issue of privacy, we ensured that all transactions made in the blockchain remain secure by utilising a decentralised digital identity, where every user connecting to the blockchain gets a unique account with a random public key. The decentralised identity allows users to own their credentials data and manage their own identities rather than have it managed by a third party.

3) Confidentiality: To help maintain confidentiality, the system will make use of asymmetric encryption technology to ensure that every access to the system is done only after authorisation. The authorisation will be a randomly generated unique token that will have to be signed by a user's private key to authenticate the client to the messaging server.

4) Availability: Our model ensures that data associated with verification and authorisation processes that are stored on the Blockchain is always available. On a per-node basis, each node replicates and updates transaction data. This means that the network will continue to function even if a node leaves it accidentally or maliciously or otherwise the node becomes inaccessible. As a result, our system will continue to operate at a high level of availability and reliability.

C. Performance analysis

We present a set of experiments to characterise the impact of our approach on wearables medical devices. Our measurements setup depends on an ESP32 with a 240MHz Dual Core CPU WROOM-32D and 4MB flash. We analysed our approach in comparison to the current security mechanisms. For this, we adopted the TLS protocol, which supports different cryptographic algorithms.

From the evaluation, we observed that the current TLS utilises a higher memory than our mechanism because it needs to allocate additional buffers. To establish a TLS session, enough free heap memory is required. A single TLS session requires around 40KB of additional heap memory. Moreover, compared to our approach, the CPU processing overhead when using TLS is also higher since cryptographic operations are involved, especially with a certificate that uses a large key length, as shown in figure 2. In addition, using TLS on the ESP32 requires a significant amount of energy. Our approach is beneficial in terms of energy consumption and significantly reduces the required energy for IoT devices.

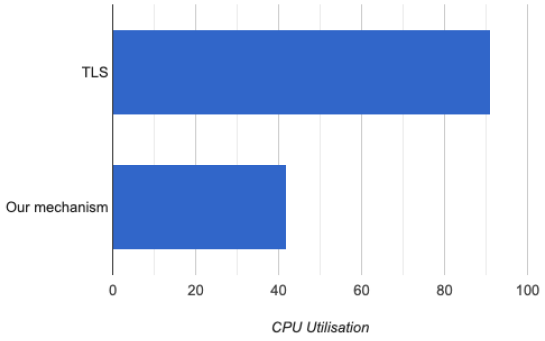

Fig. 2. **CPU overhead**

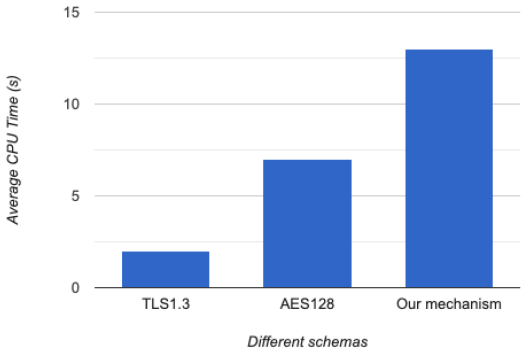

Fig. 3. **End to end delay**

To measure the overall time of establishing a secure connection, we utilised the internal time function of the microcontroller. As shown in figure 3, our approach has shown a higher execution time overhead. This is an expected issue when adopting the public Ethereum blockchain. This is due to the time needs it to finalise the transactions, which is around 13 seconds on average. However, this is a well-known issue with other real-world applications that depend on a third party to maintain trust. Still, this can be significantly enhanced

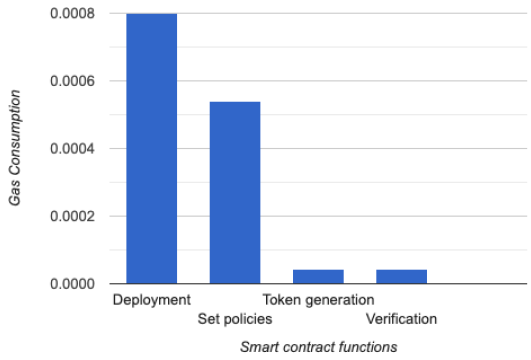

Fig. 4. **The gas cost of each event that happens in the system**

by adopting the private blockchain or utilising a reduced mining consensus that can provide immediate block finality and reduce the time needed to finals the transactions.

Moreover, any action in the Ethereum blockchain requires a certain amount of gas to send transactions and interact with the smart contract. Our result revealed that smart contract deployment is the highest cost, as shown in figure 4. Nonetheless, this cost is variant, as it depends on different parameters, such as the transaction speed and the storage required. However, it is necessary to emphasise that our implementation is based on the Rinkeby testing environment, which requires no cost as Ethereum provides free Ethers to this testing network.

X. Conclusions

In this research, a blockchain-based authentication and access control mechanism is proposed for the Internet of Healthcare Things. The paper presented a proof-of-concept design and implementation of a lightweight and secure framework for medical wearable devices. The proposed approach helps to solve privacy and security challenges across the Internet of Healthcare Things systems. It provides a privacy-preserving access control mechanism and facilitates secure users' authentication. This allows the system's users to have full control over their credentials rather than maintaining them by a third party. We have presented the solution in the form of a medical wearable sensor prototype and a mobile app that uses the Ethereum blockchain in a real data sharing control scenario. The security of our system and an attacks model have been analysed to evaluate the ability of our system to meet the security requirements of the IoT systems. Our solution showed enhancements in security and users' privacy compared to the current centralised models. In addition, we provided an analysis of the performance and the associated transactions costs. We observe that our approach provides negligible memory and CPU usage compared with the current TLS and prove suitable for resource-constrained devices. It is feasible that our approach satisfies the security requirements for IoT applications and meet future demands. We hope that our approach improves the privacy and security of users' sensitive health data. On the other hand, the proposed approach shows a significant delay due to the characteristics of the public blockchain since transactions need to be appended to the block but are still within an acceptable range. In order to improve the transactions speed and reduce the end-to-end delay, our future work would aim to evaluate different consensus mechanisms and blockchain systems, such as Hyperledger and IOTA.

References

[1] M. Javaid and I. H. Khan, "Internet of things (iot) enabled healthcare helps to take the challenges of covid-19 pandemic," *Journal of Oral Biology and Craniofacial Research*, vol. 11, no. 2, pp. 209–214, 2021.

[2] N. Tariq, A. Qamar, M. Asim, and F. A. Khan, "Blockchain and smart healthcare security: A survey," *Procedia Computer Science*, vol. 175, pp. 615–620, 2020.

[3] A. Ometov, V. Shubina, L. Klus, J. Skibińska, S. Saafi, P. Pascacio, L. Flueratoru, D. Q. Gaibor, N. Chukhno, O. Chukhno *et al.*, "A survey on wearable technology: History, state-of-the-art and current challenges," *Computer Networks*, p. 108074, 2021.

[4] S. Al-Sarawi, M. Anbar, R. Abdullah, and A. B. Al Hawari, "Internet of things market analysis forecasts, 2020–2030," in *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*. IEEE, 2020, pp. 449–453.

[5] A. Newaz, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, "A survey on security and privacy issues in modern healthcare systems: Attacks and defenses," *arXiv preprint arXiv:2005.07359*, 2020.

[6] Y. Xue, "A review on intelligent wearables: Uses and risks," *Human Behavior and Emerging Technologies*, vol. 1, no. 4, pp. 287–294, 2019.

[7] A. Nahapetian, "Side-channel attacks on mobile and wearable systems," in *2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2016, pp. 243–247.

[8] Y. Zhang, Y. Xiang, X. Huang, and L. Xu, "A cross-layer key establishment scheme in wireless mesh networks," in *European Symposium on Research in Computer Security*. Springer, 2014, pp. 526–541.

[9] K. T. Nguyen, N. Oualha, and M. Laurent, "Authenticated key agreement mediated by a proxy re-encryptor for the internet of things," in *European symposium on research in computer security*. Springer, 2016, pp. 339–358.

[10] F. Wu, X. Li, L. Xu, S. Kumari, M. Karuppiah, and J. Shen, "A lightweight and privacy-preserving mutual authentication scheme for wearable devices assisted by cloud server," *Computers & Electrical Engineering*, vol. 63, pp. 168–181, 2017.

[11] R. S. M. Joshitta and L. Arockiam, "Device authentication mechanism for iot enabled healthcare system," in *2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET)*. IEEE, 2017, pp. 1–6.

[12] F. P. Diez, D. S. Touceda, J. M. S. Cámara, and S. Zeadally, "Lightweight access control system for wearable devices," *IT Professional*, vol. 21, no. 1, pp. 50–58, 2019.

[13] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for iot," *Computers & Security*, vol. 78, pp. 126–142, 2018.

[14] H. Guo, W. Li, M. Nejad, and C.-C. Shen, "Access control for electronic health records with hybrid blockchain-edge architecture," in *2019 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2019, pp. 44–51.

[15] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," *Journal of medical systems*, vol. 40, no. 10, pp. 1–8, 2016.

[16] S. Nakamoto, "Bitcoin whitepaper," *URL: https://bitcoin. org/bitcoin. pdf-(: 17.07. 2019)*, 2008.

[17] ——, "Bitcoin: A peer-to-peer electronic cash system," Manubot, Tech. Rep., 2019.

[18] V. Buterin *et al.*, "A next-generation smart contract and decentralized application platform," *white paper*, vol. 3, no. 37, 2014.

[19] F. Ghaffari, E. Bertin, J. Hatin, and N. Crespi, "Authentication and access control based on distributed ledger technology: A survey," in *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*. IEEE, 2020, pp. 79–86.

[20] O. Standard, "Mqtt version 3.1. 1," *URL http://docs. oasis-open. org/mqtt/mqtt/v3*, vol. 1, 2014.

[21] M. Collina. (2013) Mosca : the mqtt server for node.js that can be backed up by amqp, redis, zeromq or just mqtt. [Online]. Available: http://mcollina.github.com/mosca/