Fog-based Smart Contract Platform for Wearable IoT-enabled Telemedicine

Marc Jayson Baucas and Petros Spachos
School of Engineering, University of Guelph, Guelph, ON, Canada

GLOBECOM 2023 - 2023 IEEE Global Communications Conference | 979-8-3503-1090-0/23/$31.00 ©2023 IEEE | DOI: 10.1109/GLOBECOM54140.2023.10436830

***Abstract*—Healthcare has moved towards integrating wireless technology to create and enable more services for the patients' convenience. Among the new and popular services is the formulation of wearable Internet of Things (IoT)-enabled telemedicine. However, when the number of IoT devices entering the network increases, it creates concerns about the service's ability to keep its data secure and preserve its real-time capabilities. To address these issues, in this work, we propose a fog-based IoT platform incorporating blockchain technology and smart contracts. We evaluated our design's ability to keep the real-time capabilities of wearable IoT-enabled telemedicine services through experimentation. According to the results, the introduced platform can effectively reduce the overall latency of data transactions compared to other standard network configurations. We further evaluated and observed the contributions of our design to the security of the telemedicine service. Through experimentation, we prove the feasibility of the proposed platform in addressing the highlighted issues of wearable IoT-enabled telemedicine services.**

***Index Terms*—Distributed processing, Security, Privacy, Healthcare, Blockchain, Smart contracts, Fog computing, Experiments, and Wearable IoT devices.**

I. Introduction

Telemedicine, a part of healthcare services, can benefit from incorporating Internet of Things (IoT) networks [1]. It is where medical services are deployed wirelessly through wearable IoT devices. The devices integrated into the system allow medical centers to diagnose and monitor their patient's conditions remotely [2]. Also, it expands healthcare services to remote and real-time monitoring. However, integrating wireless technology introduces issues to the security and efficiency of telemedicine services.

Telemedicine and mobile healthcare can benefit from low-cost wearable IoT devices to reduce expenses and resource allocation of medical centers [3]. The lower specifications of these devices limit the options for securing the transmitted data. As a result, there are growing concerns about the security of telemedicine services integrating IoT technology. Another problem for telemedicine can stem from the demand for faster and more efficient data transmissions when monitoring patients and administering healthcare [4]. Telemedicine is known for its advancements in allowing real-time patient monitoring over a wireless network. As a result, lower latency and efficient response times are in demand. Distance and network structure can be a factor, limiting the speed of the data transmissions due to the system deployed and served remotely.

In this work, we introduce a blockchain-based platform to improve the security of telemedicine services when sending data from its wearable devices to the medical center servers. We further propose the integration of smart contracts to allow more automative and efficient data transactions. We implemented our design on a fog-based IoT network to reinforce our decentralized approach for secure telemedicine services while maintaining their real-time efficiency.

The rest of this paper is as follows: Section II discusses the different technologies used in the platform. Section III features the proposed approach, and Section IV presents the experiments we conducted to investigate the feasibility of our platform. Finally, Section V concludes our work.

II. Background

The following section is a background study of different technologies and research related to our proposed platform.

A. Wearable IoT-enabled Telemedicine

Telemedicine systems use wearable IoT to collect and analyze the physiological data of their patients [5]. It incorporates IoT networks to deploy its services to customers wirelessly. Wearable IoT devices widen the scope of healthcare by making a more portable, flexible, and adaptive system for administering medical analysis and diagnosis. Telemedicine leveraged by wearable IoT allows healthcare centres to detect complex and chronic diseases early [6]. However, the nature of data transmissions over wireless mediums introduces issues to the system. One concern for wearable IoT-enabled telemedicine is the presence of threats to the security of the patient's data due to these devices. Aside from security, another concern is the need for real-time responsiveness of the telemedicine service.

The gap in current approaches to improving telemedicine systems incorporating wearable IoT is the focus on the device over the system. Recent research heavily invests in technology-specific optimizations rather than upgrading the service architecture. An example in [7] presents a power supply system for improving the performance and efficiency of wearable oxygen saturation monitors. Our approach differs as we plan to use blockchain technology and smart contracts to address the infrastructure of a wearable IoT-enabled telemedicine service. As a result, we are not focusing on a specific optimization to an existing wearable device but a platform that caters to general wearable IoT-based systems. Also, we look at fog-based IoT to complement the distributive structure of our incorporated technologies.

B. Permissioned Blockchain

We chose a blockchain to manage the data within the telemedicine service. Blockchain technology is a data structure that consists of data blocks formatted and linked cryptographically [8]. Its immutability and security come from its decentralized nature. Blockchains are considered unalterable due to their ability to synchronize with other instances to prove the integrity of their data. Also, blockchains benefit from the distributed architecture of fog-enabled IoT networks. Having copies of the blockchain within the different network layers ensures the security of every data transaction.

In [9], they present a cloud-based data-sharing framework reinforced using blockchain technology and deep learning for industrial healthcare systems. Our solution is different because we use a fog-based IoT network as the base of our blockchain. We chose it for its decentralized architecture to maximize the distributive protocols of the blockchain using the fog. The approaches presented focused on the general infrastructure of mobile healthcare where cost is not a constraint. We propose a fog-based platform for low-cost wearable IoT-enabled telemedicine.

We intend to keep the data within an exclusive list of servers. As a result, we chose to implement a permissioned blockchain and treat it as a hyperledger. It is a type of blockchain that does not require a proof of work (PoW) protocol to manage its nodes [10]. Since the network predetermines the servers it recognizes, the blockchain does not need to be open to the public. However, additional processing within the nodes due to the blockchain and fog devices can cause latency issues. Therefore, we propose smart contracts to automate the transaction processing within the blockchain and keep transactions in real-time.

C. Smart Contracts

A smart contract is an agreement protocol that defines the terms of a transaction between two or more users and automates its execution [11]. A smart contract is triggered when a data owner initiates a transaction defined by it. It can reduce the complexity of the authorization process of transactions within the blockchain. Since these terms are already defined, smart contracts can automate the verification of data transmissions, making intermediary processes faster.

In [12], they proposed a cloud-based data-sharing system for preserving medical data privacy using smart contracts. Our approach differs since we aim to improve the performance of telemedicine services with fog-based wearable IoT. The previous solutions present the organizational benefits of smart contract autonomy to cloud-based healthcare IoT. Our platform aims to highlight the security and efficiency improvements this technology can introduce to fog-based IoT networks.

There is a trade-off between adding blockchain technology to the fog-based IoT network and the network propagation latency as it adds more processes to the data transmission. This compromise causes a loss to its real-time capabilities. We aim to use smart contracts to reduce data transmission speeds within the fog-based IoT network blockchain while preserving the security strengths of the data structure. It can eliminate the impacts of any intermediary verification process with fog-based IoT networks [13]. Smart contracts can preserve the security of the fog network by keeping transactions secured within the blockchain.

III. Platform Overview and Design

The following section details the design of our proposed platform with its components and data flow.

A. Overview

Wearable IoT-enabled telemedicine has issues with security and latency. There is a limit to protecting patient privacy and their data due to the low-cost nature of the devices. Latency is a concern because of the remote deployment of the service. This design feature introduces distance and the wireless nature of its components as significant factors for effective service. As a result, wearable IoT-enabled telemedicine services need more secure and efficient patient data management.

Blockchains are known for their strength in securing data due to their immutable and distributive features. Integrating this technology into the telemedicine service can ensure patient data is secured while being transparent to their medical centres. We elected to use permissioned blockchains as an exclusive hyperledger of all transactions and registered devices within the healthcare network. It ensures that only trusted devices can access and manage the transmitted patient data. We chose to use a fog-based IoT network as the base architecture to support the decentralized structure of the blockchain. It allows efficient reallocation and balancing of processing loads across the network.

However, using blockchain technology with the fog-based IoT network can cause latency issues due to the processes it introduces. Intermediary fog devices and authorization protocols can slow down the transmission of patient data. As a result, there is a compromise in the real-time integrity of the telemedicine service. In response, we integrated smart contracts into our design to enable better automation and transaction management. This technology allows the network to circumvent any delays caused by increasing nodes and security checks while retaining security. Smart contracts simplify the authorization process for blockchains using pre-defined terms of approved transactions. The fog network introduces multiple nodes that the data needs to traverse to reach the server. This design can cause delays and increased latency in the transmission. Smart contracts can reduce the response time between nodes to limit the impact of these intermediary hubs on the overall speed of the data path.

B. Components

Our proposed platform has three sections: First, the cloud server. It is deployed on a laptop computer using an Intel Core i7 processor. For convenient service execution, this server runs on Ubuntu 16.04 enabled Windows 10. We implemented a REST API for the interactive web service of the server. We chose REST APIs due to their flexibility and modularity in programming and initializing. It can easily accommodate any client-server interaction or software required to test our proposed platform. We coded our web interface using Python. Its initialization and deployment were through Flask. Also, it initializes and integrates the permissioned blockchain within the functions and database of the API. The permissioned blockchain consists of blocks containing the following parameters: Index, Public Key, Timestamp, Smart Contracts, Transactions, and Previous Hash.

An index is a number assigned to each block based on the order of its creation. The public key is a hashed string that identifies each blockchain block. The timestamps indicate the time of its creation in Unix time format. The list of contracts includes any smart contracts defined within the blockchain network. The list of transactions contains any approved, executed, and stored data for tracking by the network. The previous hash is a hashed version of the block preceding the current block. For the smart contracts, each one has the identification of the devices associated with the terms of the transaction it is defining. Its execution depends on the agreement between these devices. Since we are using a permissioned blockchain, there is no need for fees or PoW. Therefore, we opted to exclude this mechanic from our smart contract design.

The second layer is the fog layer. We chose Raspberry Pi 3B's that run on a Raspbian-Jesse operating system as the fog device. Using the Pis made it easier for rapid prototyping and node replication. We chose Pis to support our low-cost approach to addressing the telemedicine issues we presented in this paper. The cloud and fog servers have a copy of the blockchain. Within it are smart contracts that contain the pre-defined terms of allowed transactions within the network. The third layer is the wearable IoT or edge layer. We chose a Samsung Galaxy Watch due to its availability and programmability. We programmed the watch in Java by using the Android Debug Bridge feature of Android Studios. The resulting WearOS application sets it to transmit data to the cloud server by passing it through the device.

C. Design Flow

Our proposed fog-based IoT network consists of three layers: the cloud, fog, and edge. Its arrangement is a hybrid of a star and a mesh topology. The end devices transmit data to the cloud server through the mesh created by the fog devices. This mesh allows the fog and the cloud to stay up-to-date with the blockchain to authorize transactions. A diagram showing the arrangement of the devices within the network is in Fig 1.

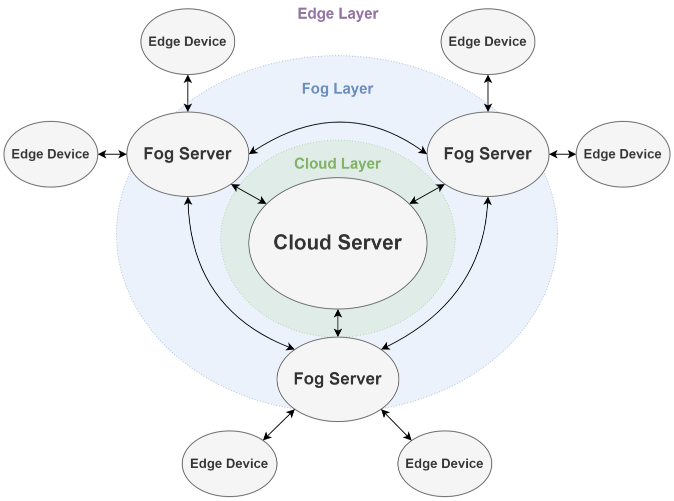


Fig. 1: Network hierarchy and arrangement of the proposed platform.

The data flow is a server-client architecture with an intermediary hub for data routing. The edge device will send the patient data to the fog nodes via wireless socket communication. Next, the fog devices will process the data packet and authorize the data based on the smart contracts within the chain. If the transaction is verified, these devices will send the information to the cloud server via a POST request to the REST API. The server will validate if the data is received and stored once the request reaches the server. Finally, the server will record the transaction into the blockchain and update all copies in the network. However, if the cloud or the fog cannot verify the integrity of the transaction, it will be discarded without further action. This flow simulates the data path of a wearable IoT-enabled telemedicine service for collecting patient data.

IV. Tests and Results

The following presents the subsections related to testing and evaluating our proposed platform.

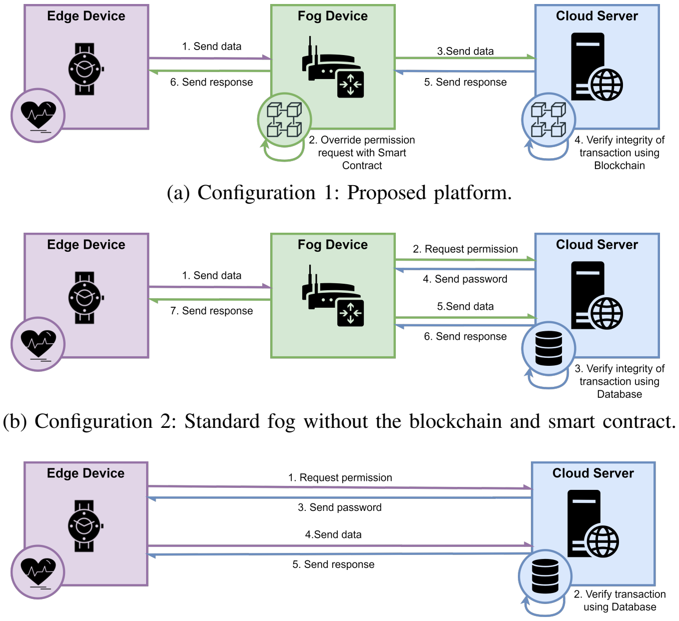
A. Testbed

We constructed an experimental testbed to simulate the behaviour of our platform carrying out a data transaction between a wearable IoT device and a cloud healthcare server. The metric we chose to test the feasibility of our design is the average latency of the patient-to-service data transaction. We model our metric as

$$T_{data} = \sum_{i=1}^{n} T_{edge} + T_{proc} + T_{cloud} \tag{1}$$

where T_{data} is the average data transaction latency, T_{edge} is the propagation time of the edge device data transmission to the cloud server, T_{proc} is the total processing time among the cloud and fog servers, T_{cloud} is the propagation time of the cloud server response back to the edge device, and n is the number of samples for each measurement.

Our experiments pit our platform against other configurations. We have three setups. First is a low-cost prototype of our proposed platform. It starts with the smartwatches sending data to the Pis. Since the Pi is local to the smartwatch, it has the smart contract shortlisted. Therefore, searching through the list to permit the data transaction is unnecessary. However, since the server is responsible for data from other fog servers, it will double-check the integrity of the transaction through the



(a) Configuration 1: Proposed platform.

(b) Configuration 2: Standard fog without the blockchain and smart contract.

(c) Configuration 3. Standard cloud without the blockchain and smart contract.

Fig. 2: The three different configurations we used in our experiments.

blockchain. Then, if verified, the server stores the data for later processing and records the transaction within the blockchain for tracking. The second configuration is a variation of our architecture. It does not have a blockchain or smart contract implemented. As a result, it will go through the authorization process using a standard database or a list of trusted device transactions. So, instead of consulting the smart contracts, the fog device first requests permission to transmit before sending over the data. The server will go through a list of database entries during this request. If the transaction is verified, it will respond with a password that the fog server will send along with the data to confirm. The third configuration is our control. It is direct data transmission from the wearable IoT device to the server. However, this does not have a blockchain. As a result, the authorization and storing process will be the same as the second configuration. However, instead of the Pi, it will be the smartwatch that will send the API request. A visual representation of the testbed configurations, their components, and their data flow is in Fig 2.

In our experiment, we observe the performance of each configuration as we increase the list's length that the cloud server will have to use for authorizing devices. In our first experiment, we will increment the chain length based on the number of smart contracts added for the setups with blockchains. As for the others, we will add a database entry to the list for every trusted transaction. This increase will simulate the effectiveness of each design as more server-and-patient transaction terms join the service. In our second experiment, we will increase the data packet size that the edge device will transmit to the server. This increase simulates the effectiveness of each configuration as data becomes more complex as the telemedicine service grows and caters to more types of physiological data and analysis. We programmed the server to do a linear search from the most recent entry to the oldest. Since we placed the correct one at the beginning of the list, the server will have to go through the entire data structure to complete the verification process. This arrangement allows us to observe the performance of each configuration at its maximum capacity and how it will affect the speed of its data transactions. This test can check if our platform can keep the latency low as the length of the database containing the trusted device transactions increases.

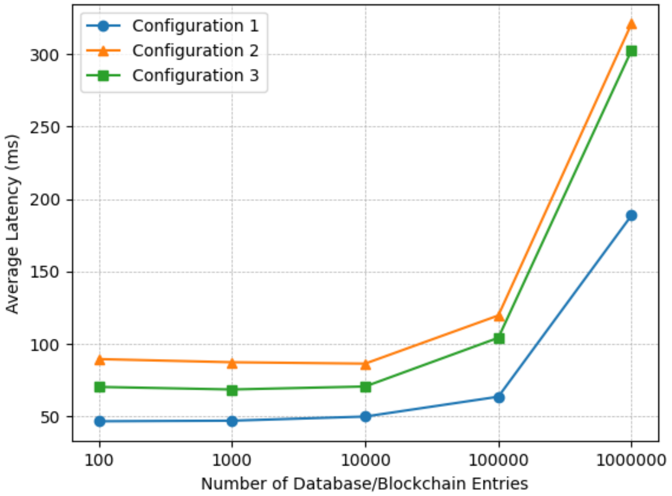


Fig. 3: Average transaction latency vs. the number of server data entries using different network configurations.

B. Average Transaction Latency Test

We tested the average transaction latency by setting up a testbed where a wearable device sends data to a cloud server. Based on the configuration, the data goes through a fog device or is sent directly to the cloud. The experiment measures the time it takes for the data to leave the watch to the moment the same device receives a response confirming the completion of the transaction. We programmed the testbed to send data continuously for 30 seconds. Next, we collected the latency value ten times and calculated the average for each configuration. Then, we increased the length of the database/blockchain by adding dummy data entries to simulate the increase of trusted devices and transactions within the service. These entries are 100, 1000, 10000, 100000, and 1000000. Finally, we compiled the resulting average latency values and placed them into a plot shown in Fig. 3.

Based on the results, we can observe that our proposed platform yielded the best performance among the configurations we tested. We can infer through the plot that adding the fog by itself cannot optimize the data path based on the performance of the second configuration compared to the third. Initially, we attributed this behaviour to the added node due to the fog device, which slows down the data flow. However, its difference from the results of the standard

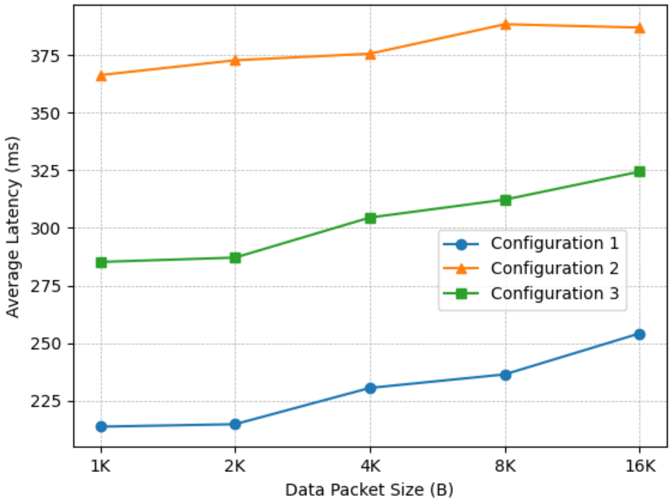


Fig. 4: Average transaction latency vs. the data packet size using different network configurations.

cloud is not too significant compared to our platform. Also, the presence of a fog device does not seem to impact our proposed design. Therefore, we can safely attribute most of our proposed platform's latency advantage to the permissioned blockchain and smart contracts in improving the speed of data flow between the edge device and the cloud server, even with an intermediary hub. This observation supports the claims of the ability of smart contracts to improve the latency of data transactions. It introduces a shortlist for devices to override any delays caused by authorizations and access permissions due to its automative features. We can observe the sustainability of our design against scaling telemedicine services that grow in their user base of trusted edge devices and local fog networks. Overall, our proposed platform shows the potential to preserve the real-time capabilities of wearable IoT-enabled telemedicine services.

C. Average Data Throughput Test

We used the same testbed to measure the average throughput of each configuration. The metric we used is the total time it takes to complete the data transaction from the edge to the cloud. We started measuring from the edge device, initiating the transaction to the cloud server and completing it by giving a final response. It is to observe the differences in data throughput for each configuration. We used packet sizes that were 1024, 2048, 4096, 8192, and 16384 B, respectively. We measured each iteration of each platform configuration three times. Each measurement was 30 seconds of continuous data transmission. We set the chain/database length to 1000000 for a more consistent comparison. Afterwards, we averaged the collected times to represent each size category for each setup. The resulting plot showing the average overhead throughput is in Fig. 4.

Based on the results, we can observe that increasing packet sizes have affected the second configuration, which is the fog-based architecture without the blockchain and smart contract. We can attribute this result to the number of hops needed to complete the data transaction. Since a cloud configuration only has two interacting nodes, the data takes fewer node hops to reach the server. However, a fog configuration would need more time to complete because there is an intermediary node that the data needs to pass through. Also, increasing the packet size further exposes this weakness because the data requires more time with each node before moving. However, we can see the advantages of adding the smart contract and blockchain as it improves the fog setup and significantly reduces the transaction time to a point where it even makes it faster than a standard cloud setup with fewer nodes to complete. As a result, the overall throughput of our proposed configuration is the best among the three. It can output the most data packets within a fixed time frame by yielding the fastest average time. We can attribute this behaviour to the smart contract speeding up data transmission in the fog device by automating the authorization process. As a result, the extra hop done by the data packet becomes less significant to the transaction time. Since we used a database/blockchain length of 1000000, we can build on the previous test results and emphasize the strengths of smart contracts and the private blockchain to the fog-based IoT network. Therefore, we can take both results and confidently claim the benefits of these technologies to improve the data transaction times within the wearable IoT-enabled telemedicine network.

D. Security Analysis

Aside from its latency, we will evaluate our design's security contributions. The blockchain can ensure the network has secure and tamper-proof storage for its transactions and trusted devices. This feature allows a more exclusive service that can protect the data of its users. It is meaningful for telemedicine services because it emphasizes patient information privacy. The immutability that the blockchain introduces can ensure that patient data will be hard to modify unless you are a trusted user. Since all transactions from the healthcare network are within it, its tamper-proof structure can prevent malicious attacks that aim to tamper with or inject harmful data within a targeted network. For instance, if a malicious user compromises one of the fog servers holding a copy of the blockchain, the network can use others to cross-reference and catch any anomalies. Also, if a malicious user aims to inject their falsified information into the transaction, the servers can verify the integrity of the source through the blockchain's historical records.

As for access control, smart contracts can ensure that only trusted devices can interact with the service and its stored data. It can introduce automative protocols that enforce secure user and server management. As a result, the network can have an easier time detecting attacks such as spoofing and impersonation using the detection layer imposed by smart contracts. For example, we can catch a malicious user who aims to spoof or impersonate an existing account by adding terms within the smart contracts to verify past transactions and the integrity of the source.

The fog architecture can improve the blockchain's and smart contracts' impact on network security by providing a decentralized structure. This structure reinforces the distributive features of each of these presented technologies. A distributive network can help alleviate network strains and prevent denial of service (DoS) attacks that overwhelm a server [14]. Overall, our platform presents a cohesive IoT network design that can improve the security of wearable IoT-enabled telemedicine services.

E. Open Issues and Future Iterations

For open issues, we recognize the limitations of our setup in scalability when accurately measuring the latency and throughput of the network as it grows. Eventually, the distributive approach will plateau in improving once the fog servers and the wearable IoT devices start hitting their technological limitations. Like parallelism in computers, reallocating resources is only as good as its worst thread. As for the wearables, power consumption and portability are some aspects not touched by this paper but are still a concern in maintaining an effective and sustainable remote patient monitoring service.

Therefore, for future iterations, we plan on incorporating a more diverse selection of wearable devices to increase the scope of our platform. With more devices, we can better understand which part of the edge layer needs improving. Aside from optimizing the edge, we look to add other techniques like federated learning [15] to complement and upgrade our fog design's distributive capabilities and security. We can use it to reinforce our platform's access layer, improving its defences and verification efficiency. Since our current work is limited to the blockchain aspect of the architecture, adding other technologies and approaches that complement the fog-IoT network can benefit our overall platform.

V. Conclusion

We present a platform that addresses the issues of wearable IoT-enabled telemedicine services in security and data transaction latency. We use the permissioned blockchain's immutability and distributive features to secure the telemedicine service's data. Next, we incorporate smart contracts to automate access verification, preserving the real-time advantage of telemedicine services. Lastly, we implement these technologies within a fog-based IoT network architecture to reinforce their decentralized structures.

We evaluated the feasibility of our proposed platform by measuring its averaged data transaction latency. We compared it against other standard network configurations. The results showed that our platform preserves and improves the real-time capabilities of fog-based wearable IoT-enabled telemedicine services. We also evaluated the security contributions of our proposed design. The blockchain introduces immutability. Also, smart contracts complement it with automation. The result is a reinforced design that can keep data within the network tamper-proof and its authorization process sustainable.

However, there are still open issues like limitations in scalability and fog technology. As a result, we aim to address these concerns by optimizing the different technologies within the proposed platform and incorporating other techniques, such as deep learning, to upgrade the architecture. Overall, our evaluations presented the feasibility of our proposed platform in addressing the security and real-time concerns of wearable IoT-enabled telemedicine services.

References

[1] S. Misra, S. Pal, N. Pathak, P. Deb, A. Mukherjee, and A. Roy, "i-avr: Iot-based ambulatory vitals monitoring and recommender system," *IEEE Internet of Things Journal*, vol. 10, no. 12, pp. 10318–10325, 2023.

[2] T. Adiono, N. Ahmadi, C. Saraswati, Y. Aditya, Y. Yudhanto, A. Aziz, L. Wulandari, D. Maranatha, G. Khusnurrokhman, A. Riadi, and R. Sudjud, "Respinos: A portable device for remote vital signs monitoring of covid-19 patients," *IEEE Transactions on Biomedical Circuits and Systems*, vol. 16, no. 5, pp. 947–961, 2022.

[3] Y. Yang, H. Wang, R. Jiang, X. Guo, J. Cheng, and Y. Chen, "A review of iot-enabled mobile healthcare: Technologies, challenges, and future trends," *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 9478–9502, 2022.

[4] A. Moglia, K. Georgiou, B. Marinov, E. Georgiou, R. Berchiolli, R. Satava, and A. Cuschieri, "5g in healthcare: From covid-19 to future challenges," *IEEE Journal of Biomedical and Health Informatics*, vol. 26, no. 8, pp. 4187–4196, 2022.

[5] J. Leitner, A. Behnke, P. Chiang, M. Ritter, M. Millen, and S. Dey, "Classification of patient recovery from covid-19 symptoms using consumer wearables and machine learning," *IEEE Journal of Biomedical and Health Informatics*, vol. 27, no. 3, pp. 1271–1282, 2023.

[6] C. Wu, S. Wang, Y. Su, T. Hsieh, P. Chen, Y. Cheng, T. Tseng, W. Chang, C. Su, L. Kuo, J. Chien, and F. Lai, "A precision health service for chronic diseases: Development and cohort study using wearable device, machine learning, and deep learning," *IEEE Journal of Translational Engineering in Health and Medicine*, vol. 10, pp. 1–14, 2022.

[7] R. Álvarez González, E. González-Campos, N. Quiroz-Hernández, and A. Sánchez-Gálvez, "Three-stage power supply system model for a wearable iot device for covid-19 patients," *IEEE Embedded Systems Letters*, vol. 15, no. 2, pp. 61–64, 2023.

[8] K. Agyekum, Q. Xia, E. Sifah, C. Cobblah, H. Xia, and J. Gao, "A proxy re-encryption approach to secure data sharing in the internet of things based on blockchain," *IEEE Systems Journal*, vol. 16, no. 1, pp. 1685–1696, 2022.

[9] R. Kumar, P. Kumar, R. Tripathi, G. Gupta, A. Islam, and M. Shorfuzzaman, "Permissioned blockchain and deep learning for secure and efficient data sharing in industrial healthcare systems," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 11, pp. 8065–8073, 2022.

[10] H. Chen, Z. Chen, Y. Cheng, X. Deng, W. Huang, J. Li, H. Ling, and M. Zhang, "A provable softmax reputation-based protocol for permissioned blockchains," *IEEE Transactions on Cloud Computing*, vol. 11, no. 1, pp. 1065–1077, 2023.

[11] M. Muneeb, Z. Raza, I. Haq, and O. Shafiq, "Smartcon: A blockchain-based framework for smart contracts and transaction management," *IEEE Access*, vol. 10, pp. 23687–23699, 2022.

[12] M. Wang, Y. Guo, C. Zhang, C. Wang, H. Huang, and X. Jia, "Medshare: A privacy-preserving medical data sharing system by using blockchain," *IEEE Transactions on Services Computing*, vol. 16, no. 1, pp. 438–451, 2023.

[13] T. Hewa, A. Braeken, M. Liyanage, and M. Ylianttila, "Fog computing and blockchain-based security service architecture for 5g industrial iot-enabled cloud manufacturing," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 10, pp. 7174–7185, 2022.

[14] M. Baucas, P. Spachos, and K. Plataniotis, "Public key reinforced blockchain platform for fog-iot network system administration," *IEEE Internet of Things Journal*, pp. 1–1, 2021.

[15] M. Baucas and P. Spachos, "Federated kalman filter for secure iot-based device monitoring services," *IEEE Networking Letters*, vol. 5, no. 2, pp. 91–94, 2023.