Private Blockchain-Based Wireless Body Area Network Platform for Wearable Internet of Thing Devices in Healthcare

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

***Abstract*—In recent years, healthcare systems have included the Internet of Things (IoT) technology in their services, such as in remote patient monitoring systems. Wearable IoT devices can provide information regarding the patient's health that are accurate and time-sensitive. However, vulnerabilities are evident as more IoT devices connect to the network. For healthcare services, the security of patient data is an issue. At the same time, with real-time data transmissions, the network runs into manageability concerns. In this work, we propose a private blockchain-based Wireless Body Area Network (WBAN) platform to aid wearable IoT devices in healthcare services. We chose this blockchain technology due to its strengths in security. Then, we enable a distributive architecture using WBANs to introduce a decentralized configuration that can ensure privacy among wearable IoT devices within the network. To evaluate the feasibility of the proposed platform in terms of latency and throughput, we conducted experiments with several wearable IoT devices. The results show that integrating a WBAN to create a fog server improves the network performance with an increasing number of IoT devices and packet size. Also, the blockchain showed its ability to address security threats in healthcare services. We evaluate our proposed platform through a performance test and a STRIDE threat model, and we prove its feasibility in improving the security and manageability of wearable IoT devices in healthcare.**

***Index Terms*—Security, Fog computing, Pervasive and Wearable computing, Testbed, Experiments.**

I. Introduction

Healthcare industries have started introducing more complex and compact technologies into their services [1]. One of the most popular approaches is integrating the Internet of Things (IoT) through wearable devices for monitoring and diagnosing their patients [2]. However, there is a caveat in the private patient data that these, mainly wireless, technologies collect and transmit [3]. Proper network security is required to keep this information secure. Due to its high volume, the manageability of the data within the network is also an issue. Most medical centers use more than one technology or service for effective diagnosis and continuous patient monitoring [4]. Therefore, there is a need for a better means of securing and managing patient data.

In this work, we propose a blockchain-based Wireless Body Area Network (WBAN) platform to address the security and manageability issues in wearable IoT devices in healthcare. We use private blockchain technology to address these security issues for its strengths in keeping data tamperproof and harder to modify with its decentralized properties. We also use a WBAN architecture to rearrange the network structure under more manageable and distributive conditions. This structure can reduce the issues in data congestion for easier process reallocation and load management. We evaluate the proposed platform through experimentation with smartwatches, smartphones, and wearable prototypes.

The organization of the rest of the paper is as follows: We discuss the related works in Section II. In Section III, we introduce our platform and present the components we used to construct and test it, and we highlight the different motivations and our choices to implement the proposed design. In Section IV, we discuss the experimental results and insights. In Section V are the conclusions of this work.

II. Related Works

Healthcare industries have adopted wearable IoT devices into their services [5]. A popular approach is the remote patient monitoring systems. With this service, medical centers can manage their physical resources better and observe patients without being present in a clinic [6]. Healthcare centers provide a wireless wearable IoT device for the patient to enable this monitoring system. The technology is low-cost and compact to keep the service affordable and modular. As a result, these devices are not optimized for complex processes. Also, these devices need to be worn by patients frequently to ensure constant monitoring [7]. However, wearable IoT devices in healthcare deal with private patient data. If left unprotected, these data transmissions are prone to malicious attacks [8]. Hence, the data also needs to be kept secure. In this work, we use blockchain technology to create a platform that addresses this security issue.

A blockchain is a data structure composed of cryptographically linked blocks [9]. It is known for its immutable and decentralized architecture. As a result, blockchains can ensure that information is harder to modify with multiple control nodes with authority over the network. Also, its decentralized structure allows several backup locations to become more tamperproof. Blockchains have built-in protocols for efficient automation, making it a sustainable option instead of simpler authentication and security schemes. There are two main classifications of blockchains; public and private [10]. These two fundamental types are mainly classified based on how they grant access to the device. Conventional public blockchains use a trustless consensus protocol via proof-of-work (PoW)

ICC 2023 - IEEE International Conference on Communications | 978-1-5386-7462-8/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICC45041.2023.10278610

to authenticate their users. It provides a complex algorithm that requires processing power from the user to complete before being given access. A conventional private blockchain uses a trusted protocol [11]. Instead of using PoW, most implementations hold a ledger that identifies its authorized devices.

In [12], they proposed a decoupled private blockchain approach for regulating the user data within an edge IoT-based healthcare monitoring. Another example is in [13]. They presented a blockchain implementation that leverages edge computing creating fast data processing for healthcare applications. Our design differs by emphasizing a fog-based and distributive approach. We elected to use a conventional private blockchain due to the expected devices in our platform. Since wearable devices in IoT-based healthcare are usually low-cost, they will not have the processing capabilities to do PoW [14]. Therefore, we use a pre-defined ledger of trusted devices within the blockchain. This choice saves power consumption, which is crucial for these wearable devices. Another difference in our design is that we incorporate WBAN technology with our blockchain approach to improve the overall design structure.

A WBAN is a type of network that scopes a small area, which is usually around a person [15]. Although it cannot support a large-scale service due to capacity issues, it can create an exclusive network that limits those that can access it. As a result, it offloads processes to a local server for pre-processing [12]. Also, it can keep the information exclusive to each group of users. We chose to use this type of network for its potential contributions to the manageability and security of the overall healthcare network. With the WBAN, we add local servers to its architecture [16]. As a result, the distributive fog-based structure minimizes the network congestion caused by overloading the cloud server. Also, it reduces the total number of endpoints connected to the server, which lessens the network traffic and improves the manageability of the overall IoT service.

In [17], they proposed an IoT-based system for automated health monitoring and surveillance in response to the impact of the pandemic on in-person check-ups. Another proposed design is in [6]. Their framework is a fog-centric implementation aiming to improve the monitoring of body vitals in the health and fitness industry.

These works focus on remotely locating a fog device around a cluster of users for their implementations, while the designs aimed more at its analytical capabilities than its security. Our proposed platform is also fog-centric. However, the proposed platform differs by having the fog servers closer to each user and creating a better exclusive network through the WBAN. Also, we incorporate a private blockchain to reinforce the network's security. The proposed design focuses on providing better data protection for wearable IoT devices in healthcare.

III. Platform Design

The following sections highlight our proposed design and its components.

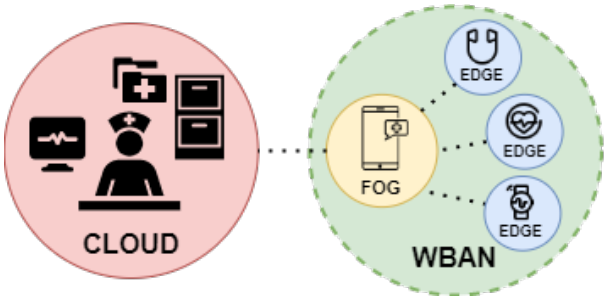


Fig. 1: Network architecture and hierarchy of our proposed platform.

A. Overview

We propose a blockchain-based WBAN platform to address security and manageability issues. The proposed design combines a private blockchain and a WBAN architecture to create a system that regulates the data for the patient. By utilizing the tamperproof and decentralized capabilities of the blockchain, we implement a security administrator for the network. Also, we keep the data and devices exclusive to the user by taking the limiting scope and unique architecture of the WBAN. As a result, patient information is secure while the overarching healthcare service is more manageable.

We design our platform to be small-scale to reflect a minimal approach to addressing the issues presented in this work. A diagram showing the network architecture and hierarchy of the proposed platform is in Fig. 1. The assigned central server manages all the wearable IoT devices of the patient. Our design uses an Android smartphone device that serves as the fog server and regulates all the data for the patient. It will be the only device communicating with the central server. This hierarchy establishes a mini WBAN around the patient, with the smartphone as the local fog server. Also, we placed the private blockchain within the fog device. The fog server will treat it as a hyperledger that authorizes data transmissions from trusted wearable IoT devices.

The communication parameters of the proposed approach are WiFi 2.4GHz and socket programming. A diagram showing the data flow within the platform as the wearable IoT devices send data to the cloud server is in Fig. 2. First, wearable IoT devices initiate the data transmission to the fog server. Each local server confirms if the source is trusted using the private blockchain. If the fog authorizes the data, it forwards the information to the cloud for storage. Otherwise, the data is not received, and users do not gain access.

B. Components

Our proposed platform has three main components; the cloud server, the fog device, and the edge devices. First, the cloud server is used mainly for storage which will house all the data from each patient. It represents the healthcare center where all data is collected. We used a standard personal computer with an Intel® Core™ i7-6500U CPU @ 2.59 GHz processor as the main server. It also contains a copy of the blockchain for cross-referencing data and verifying sources.

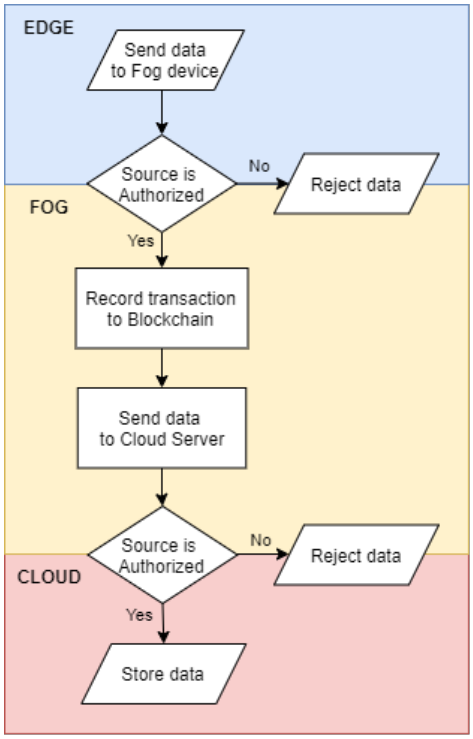


Fig. 2: Logic flow diagram of the platform as edge device sends data to the cloud server.

Due to its programmability and processing power, we used an LG Nexus 5 smartphone for the fog server. The phone uses an Android SDK 4.4 API 19 KitKat as its operating system, which is a popular OS and available to more than 98% of Android-based smartphones. Along with its vast open-source library, we wrote a script that manages the data between the wearable IoT devices and the fog server.

We programmed the private blockchain using Python. It is a chain class composed of block classes/objects linked cryptographically by hashing an instance of the previous block and storing it as a variable on the current block. The server that holds the private blockchain will initialize it by generating a base block containing a list of device IDs allowed to transmit and access the data within the cloud server. Other variables initialized along each block are an ID, a list of transactions, and a timestamp of its generation. We placed the private blockchain in the fog device to regulate the connecting wearable IoT devices and handle the incoming and outgoing data. It contains a function that will check the IDs of each data transmission. Then, it confirms if the source is a trusted device. The server denies the transaction if the data source is unregistered within the blockchain. Otherwise, it authorizes the data transmission and stores the received information in its database. Also, it records the transaction within its ledger to keep a historical record.

For the edge devices, we used a combination of Raspberry Pi 3 B's and Samsung Galaxy Watch 4's to provide the data simulating the collected patient information. Each IoT device is programmed to transmit data to the local server to simulate a physiological sensor monitoring a patient. The fog device then verifies the user against the ledger in the blockchain. If authorized, it permits the data transaction. Finally, the database within the cloud server stores the data.

IV. Results and Discussion

We conducted experiments to investigate and evaluate the feasibility of our design in terms of security and manageability.

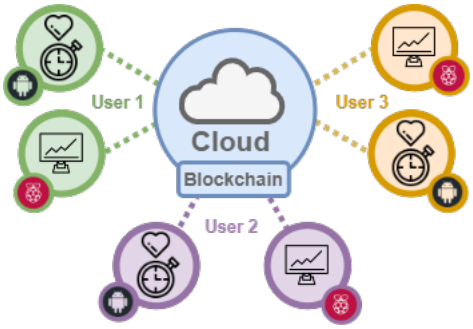
A. Experimental Design and Testbed

We examined the feasibility of our proposed platform under small-scale conditions. Aiming for large-scale conditions presents challenges in evaluating our approach. It requires more hardware and measurements to do the simulations. When modelling large-scale applications, there is a need for more data sources to represent the system effectively. Also, evaluating a design with the maximum requirements can make benchmarking more difficult due to wearable technologies upgrading frequently. A small-scale approach makes it easier to establish a minimum benchmark in addressing the issues presented by this work.

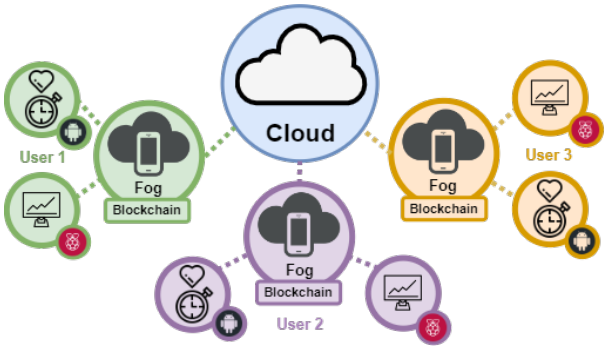
The testbed has a central cloud server using the personal computer to receive the transmitted data. Then, around it will be Android phones representing the fog devices. These devices will function as local servers. They will regulate the data from edge devices. We connected each smartphone to a pair of data sources to simulate this part of the network. These sources are a Raspberry Pi and a Samsung Galaxy Watch 4. We arbitrarily chose this arrangement to represent a user having a wearable IoT device providing their physiological data.

To examine the feasibility of this platform in terms of manageability, we focused on latency and throughput. We use these variables as the metrics for discussion. We compare our configuration with a network architecture that removes our fog component. Instead, it has IoT devices send data directly to the cloud. This configuration represents the standard structure of a cloud-centric network. Its cloud server will serve as the focal point of operations. Also, the smartwatches and the Pis will be the edge devices that provide data to the cloud and subscribe to its services. We moved the private blockchain to the cloud since the fog is not in this configuration.

We compare these configurations when managing three users, as shown in Fig. 3. The trade-off between these is control and potential security over process reallocation and server workload. The cloud-based implementation focuses all of its resources in the cloud, keeping data aggregated into one space. Although this helps centralize data collection and security, it forces the cloud to be the only server that manages and secures its data. The fog-based implementation enables process reallocation and distribution of workload across the network. However, adding local servers reduces the control and security over the data from the cloud. That is why we proposed using blockchain technology and its distributive and immutable design to compensate for and potentially improve it in the fog-based IoT network.



(a) Standard Cloud-based IoT configuration.



(b) Our Fog-based IoT configuration.

Fig. 3: Two configurations, (a) a standard cloud-based IoT and (b) our proposed fog-based IoT.

B. Security Evaluation

This platform aims to address the security of wearable IoT devices in healthcare. To evaluate our design, we use a modelling methodology to analyze it. The model that we chose to use is STRIDE. It is a threat model that analyzes the strengths and weaknesses of a design against six categories [18]. These categories are: i) Spoofing, ii) Tampering, iii) Repudiation, iv) Information Disclosure, v) Denial of Service, and vi) Elevation of Privilege. We selected this model because it can identify vulnerabilities and highlight risks in the design [19]. Also, the threats used by this model are well-known sources of security and manageability issues of IoT-based services in healthcare, education, home, and vehicles [20]. Therefore, by evaluating our design against this model, we can further support the feasibility of our platform. The following enumerates our analysis using STRIDE:

i) Spoofing - It is the process of impersonating an authorized user to access the network. This malicious attack exposes architecture vulnerabilities making user information not secure. Our platform can use the blockchain to hide user data behind an encrypted wall. It will protect the data from leaks cryptographically. Also, with the WBAN architecture, the range of detecting the network is small. Since the radius of its scope covers the area around the person, the malicious attacker would have to stand next to them to request access. This design provides a defence against spoofed users by only considering connecting devices within a very close range. With the private blockchain keeping the ledger secure and the WBAN having a small scope, our platform presents good defences against spoofing. Also, our design reduces the likelihood of tampering by connecting devices already filtered by the fog. However, this is not absolute protection against this threat. Therefore, future iterations can include more methods that reinforce the security of user information around the fog. An option is adding a second level of encryption to make access requests more complex.

ii) Tampering - It is the process of changing the contents of a data structure without authorization. Users who have access to the network can transmit data to the fog device. As previously discussed, our platform has the means to defend against spoofing. Obtaining access to the network is harder. Also, the server can detect unauthorized changes due to the tamperproof private blockchain. This advantage makes the data within the network immutable and secures it against these threats. As a result, it is more difficult to modify the data. Also, due to the fog, our architecture is decentralized. Therefore, it can detect tampering earlier. As a result, the central server is better protected from these attacks. Therefore, our platform has a built-in defence against tampering due to the private blockchain. Further iterations could also include a detection layer for faster response times against this attack.

iii) Repudiation - It is the state where the data structure can verify transactions within it. Exchange within the network is repudiated if the destination is confirmed. With our platform, repudiation is made possible with the blockchain. It is the one that will check all data transactions between the Android device and the Pis. Again, the central server defended better with earlier detection along the hierarchy. This design further improves the manageability of the network by reducing the number of vulnerabilities that can reach the server. Therefore, it can verify if all the information going in and out of the WBAN is authorized. As a result, changing any information within these transactions will be easier to catch with the blockchain.

iv) Information Disclosure - The most sensitive data that need protection is user information. The blockchain relies on these to authorize devices that attempt to communicate within the WBAN. This threat analysis exposes a vulnerability in the design. Further reinforcement of the network ledger is required to protect this information. Like the analysis from the spoofing threat, future iterations could include a better means of keeping this data structure secure.

v) Denial of Service (DoS) - It is an attack where a network is rendered unable to function. This service failure is due to an overwhelming number of devices attempting to access it. Since the platform uses a WBAN, its area is limited, which naturally reduces the entry points of location-based DoS attacks. Also, this keeps the central server safe by limiting the endpoints that talk to the

cloud. However, malicious attackers can still impersonate known devices. As a result, the network is still vulnerable. Although not absolute, our design can defend against this threat around the fog. Therefore, future interactions can implement rate limiters for the Android device to reinforce it. This addition ensures that incoming access requests are regulated.

vi) Elevation of Privilege - Our current design only recognizes two privilege levels. The device is either allowed access or not. Only the blockchain can decide which user is allowed access. Therefore, tampering with this list is the only way a malicious account can elevate its privilege. Based on our previous analysis of tampering and spoofing, our design shows promise in its defences against tampering. The only means of changing the blockchain is to overwrite it before the network initializes the application. Therefore, we can deny unauthorized changes to keep the ledger secure against unwanted elevation of privilege while the application runs. Future iterations can include a protocol that only allows changes to the list of authorized users through validated patches from the central server.

C. Throughput and Latency Evaluation

The first evaluation was for the throughput and latency of our design under small-scale conditions. As mentioned, we had two configurations. The first is our platform which uses a fog-based IoT network. Next is the control variable with a standard cloud-based IoT network arrangement. Each architecture was tested by having the devices send data to the server for one minute. We obtained the average latency by measuring the instantaneous response time of the cloud for each packet sent.

There were multiple iterations of each measurement where the user count varied from 1, 3, and 5. To evaluate the throughput, we tested different sizes of the packets in each iteration at 128, 256, 512, and 1024 bytes of data. A diagram comparing the response average time of the cloud server to each configuration at varying numbers of users and data sizes is in Fig. 4. According to the experimental results, the platform yielded lower latencies with our fog configuration. This behaviour means that the cloud server is more responsive to the fog configuration than the standard cloud as more devices connect. As a result, our proposed design shows potential for alleviating manageability concerns within the network regarding latency. In terms of increasing data sizes, the average response time of our configuration was lower.

A plot showing a closer analysis of the throughput using the iteration with five users is in Fig. 5. When the size of the transmitted data increased, our configuration performed better by showing little change in the response time. However, the standard cloud server jumps in this value with the change in packet size. Compared to the cloud configuration, ours was better at catering to increasing data sizes. This trend shows that more data can be allowed in each transmission. Therefore, our design can optimize the network architecture.

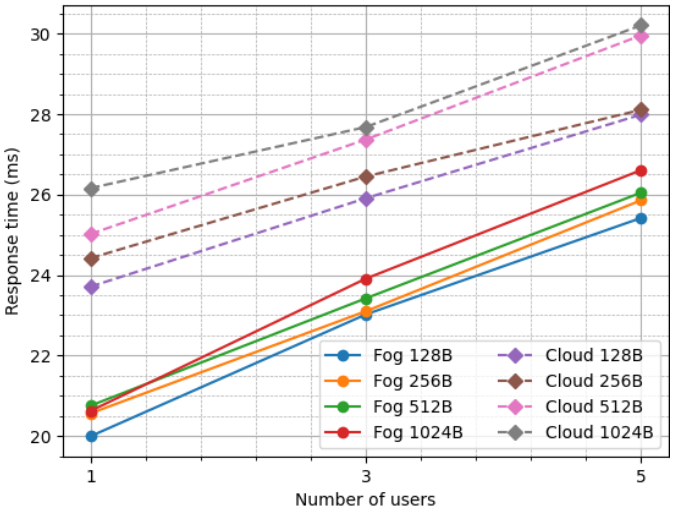


Fig. 4: Server response time comparison of fog and cloud configurations with varying numbers of users and packet size.

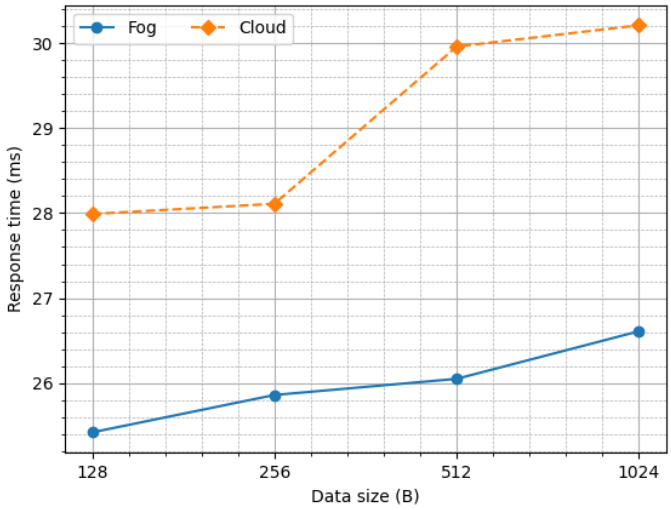


Fig. 5: Server response time comparison of fog and cloud configurations with varying data sizes for the five user iterations.

Also, providing space for encrypting methods reinforces the security of the data within the packet. With these observations, we can see that our configuration shows the potential alleviating some manageability concerns of the network in terms of throughput as the volume of transmitted data increases. Overall, the results show how our proposed fog configuration for the platform improves the ability to scale the IoT network regarding latency and throughput.

D. Discussion

Overall, the private blockchain shows great defences regarding security against most of the threats in this model. The platform data is immutable to a certain degree because of the blockchain. It is secure unless there is direct tampering in the application. Also, the WBAN can mitigate most location-based attacks due to its limited area scope. The network can detect unknown users because it grants access through

the blockchain. Also, it can limit the amount of data being disclosed by creating levels of access to keep sensitive data written and protected. With the cryptographical capabilities of blockchain technology, keeping data secure and tamperproof makes it convenient.

Based on the experiments, introducing the fog device via the Android phone shows the potential alleviating manageability concerns of the network in terms of latency and throughput. With an intermediary medium that preprocesses the data before it reaches the server, we can reduce the number of endpoints that the network needs to manage. With lesser endpoints, there is an improvement in the latency and throughput of the network. Also, the volume of data is less likely to overwhelm the server. As for security, these attacks are less likely to reach the central server with another defence layer that detects these threats earlier. Also, we can add measures that increase the data flow security of the network with a more capable processing point. As a result, it limits the need for processes that overwhelm edge devices and disrupt data collection. Therefore, we can see through these tests and evaluations that using the blockchain with the WBAN architecture is feasible in terms of security and manageability.

V. Conclusions

We proposed a platform to improve the security and manageability of wearable IoT devices in healthcare. To reinforce the network, we elected to integrate a private blockchain. It makes data secure and immutable using its tamperproof and decentralized structure. Meanwhile, to improve the manageability of wearable IoT devices in healthcare, we used the architecture of WBANs. This design choice introduces a fog layer to the network. As a result, we can reallocate processes to a local server, which reduces the overall strain on the main.

We evaluated the feasibility of this design in terms of security and manageability. First, we used a STRIDE threat model to investigate how secure is our blockchain-based platform. The results show how integrating private blockchains and WBANs into the platform can address the threats provided by the evaluation. Then, we tested its latency and throughput to prove if it makes the IoT network more manageable. Our fog-based IoT network, created by integrating the WBAN architecture, was compared against a standard cloud-based configuration. The results revealed improved manageability in our design with better performance based on server response time and data overhead regulation.

References

[1] Mohammad Nuruzzaman Bhuiyan, Md Mahbubur Rahman, Md Masum Billah, and Dipanita Saha, "Internet of things (iot): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10474–10498, 2021.

[2] Francisco Airton Silva, Tuan Anh Nguyen, Iure Fé, Carlos Brito, Dugki Min, and Jae-Woo Lee, "Performance evaluation of an internet of healthcare things for medical monitoring using m/m/c/k queuing models," *IEEE Access*, vol. 9, pp. 55271–55283, 2021.

[3] Hadi Habibzadeh, Karthik Dinesh, Omid Rajabi Shishvan, Andrew Boggio-Dandry, Gaurav Sharma, and Tolga Soyata, "A survey of healthcare internet of things (hiot): A clinical perspective," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 53–71, 2020.

[4] Mostafa Haghi, Sebastian Neubert, Andre Geissler, Heidi Fleischer, Norbert Stoll, Regina Stoll, and Kerstin Thurow, "A flexible and pervasive iot-based healthcare platform for physiological and environmental parameters monitoring," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5628–5647, 2020.

[5] Ke Wang, Chien-Ming Chen, Zhuoyu Tie, Mohammad Shojafar, Sachin Kumar, and Saru Kumari, "Forward privacy preservation in iot-enabled healthcare systems," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 3, pp. 1991–1999, 2022.

[6] Afzaal Hussain, Kashif Zafar, and Abdul Rauf Baig, "Fog-centric iot based framework for healthcare monitoring, management and early warning system," *IEEE Access*, vol. 9, pp. 74168–74179, 2021.

[7] Vinicius F. Rodrigues, Rodrigo R. Righi, Cristiano A. Costa, Rodolfo S. Antunes, Rodrigo Bazo, Eduardo S. Reis, Lucas A. Seewald, Luis G. S. Junior, and Björn M. Eskofier, "Healthstack: Providing an iot middleware for malleable qos service stacking for hospital 4.0 operating rooms," *IEEE Internet of Things Journal*, vol. 9, no. 19, pp. 18406–18430, 2022.

[8] Waseem Iqbal, Haider Abbas, Mahmoud Daneshmand, Bilal Rauf, and Yawar Abbas Bangash, "An in-depth analysis of iot security requirements, challenges, and their countermeasures via software-defined security," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10250–10276, 2020.

[9] Partha Pratim Ray, Dinesh Dash, Khaled Salah, and Neeraj Kumar, "Blockchain for iot-based healthcare: Background, consensus, platforms, and use cases," *IEEE Systems Journal*, vol. 15, no. 1, pp. 85–94, 2021.

[10] Mohammad Wazid, Ashok Kumar Das, Sachin Shetty, and Minho Jo, "A tutorial and future research for building a blockchain-based secure communication scheme for internet of intelligent things," *IEEE Access*, vol. 8, pp. 88700–88716, 2020.

[11] Marc Jayson Baucas, Petros Spachos, and Konstantinos N. Plataniotis, "Public-key reinforced blockchain platform for fog-iot network system administration," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22366–22374, 2022.

[12] Gagangeet Singh Aujla and Anish Jindal, "A decoupled blockchain approach for edge-envisioned iot-based healthcare monitoring," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 2, pp. 491–499, 2021.

[13] Zhongxing Ming, Mingzhao Zhou, Laizhong Cui, and Shu Yang, "Faith: A fast blockchain-assisted edge computing platform for healthcare applications," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 12, pp. 9217–9226, 2022.

[14] Leili Soltanisehat, Reza Alizadeh, Haijing Hao, and Kim-Kwang Raymond Choo, "Technical, temporal, and spatial research challenges and opportunities in blockchain-based healthcare: A systematic literature review," *IEEE Transactions on Engineering Management*, vol. 70, no. 1, pp. 353–368, 2023.

[15] Enas Selem, Mohammed Fatehy, and Sherine M. Abd El-Kader, "mobthe (mobile temperature heterogeneity energy) aware routing protocol for wban iot health application," *IEEE Access*, vol. 9, pp. 18692–18705, 2021.

[16] Cheng Guo, Pengxu Tian, and Kim-Kwang Raymond Choo, "Enabling privacy-assured fog-based data aggregation in e-healthcare systems," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 3, pp. 1948–1957, 2021.

[17] Seyed Shahim Vedaei, Amir Fotovvat, Mohammad Reza Mohebbian, Gazi M. E. Rahman, Khan A. Wahid, Paul Babyn, Hamid Reza Marateb, Marjan Mansourian, and Ramin Sami, "Covid-safe: An iot-based system for automated health monitoring and surveillance in post-pandemic life," *IEEE Access*, vol. 8, pp. 188538–188551, 2020.

[18] Xuan Hu, Debin Cheng, Junming Chen, Xiantao Jin, and Bo Wu, "Multiontology construction and application of threat model based on adversarial attack and defense under iso/iec 27032," *IEEE Access*, vol. 10, pp. 117955–117972, 2022.

[19] Timo Klein, Tanja Fenn, Anett Katzenbach, Heiner Teigeler, Sebastian Lins, and Ali Sunyaev, "A threat model for vehicular fog computing," *IEEE Access*, vol. 10, pp. 133256–133278, 2022.

[20] Nivedita Mishra and Sharnil Pandya, "Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review," *IEEE Access*, vol. 9, pp. 59353–59377, 2021.