Developing a Patient-Centric Healthcare IoT Platform with Blockchain and Smart Contract Data Management

Duc B. T.[1], Trung P. H. T.[2], Trong N. D. P.[3], Phuc N. T.[4], Khoa T. D.[5],
Khiem H. G.[6], Nam B. T.[7], Bang L. K.[8]
Nguyen Tat Thanh University, Ho Chi Minh City, Viet Nam[1]
FPT University, Can Tho City, Viet Nam[2,3,4,5,6,7,8]

Abstract—**The Internet of Things (IoT) has been rapidly integrated into various industries, with healthcare emerging as a key area of impact. A notable development in this sector is the IoHT-MBA system, a specialized Internet of Healthcare Things (IoHT) framework. This system utilizes a microservice approach combined with a brokerless architecture, efficiently tackling issues like data gathering, managing users and devices, and controlling devices remotely. Despite its effectiveness, there's a growing need to improve the privacy and control of patient data. To address this, we propose an enhanced version of the IoHT-MBA system, incorporating blockchain technology, specifically through the use of Hyperledger Fabric. This integration aims to create a more secure, transparent, and patient-centric data management platform. The system enables patients to oversee their peripheral devices, such as smartphones and sensors. These devices are integrated as part of the edge layer of the IoHT, contributing to a decentralized storage service. In our model, data is primarily retained on user devices, with only summarized data being communicated to service providers and recorded on the blockchain. This approach significantly boosts data privacy and user control. Access to user data is strictly regulated and must align with the patient's privacy conditions, which are established through smart contracts, thus providing an additional layer of security and transparency. We have conducted an evaluation of our blockchain-enhanced platform using key theories in microservice and brokerless architecture, such as Round Trip Time and Broken Connection Test Cases. Additionally, we've performed tests on data generation and queries using Hyperledger Caliper. The results confirm the strength and efficiency of our blockchain-integrated system in the healthcare IoT domain.**

Keywords*—*Medical test result; blockchain; smart contract; NFT; Ethereum; Fantom; polygon; binance smart chain

I. INTRODUCTION

The landscape of the Internet of Things (IoT) has broadened substantially, now covering sectors including smart urban development, medical care, logistical supply chains, industrial processes, and agrarian practices. Forecasts indicate that by the year 2023, IoT-connected devices globally are expected to escalate to 43 billion, a significant increment from the figures recorded in 2018 [1]. Concurrently, investments in IoT infrastructure are anticipated to witness an annual growth of 13.6% up to the year 2022 [1]. Notably, the healthcare industry is a major adopter, constituting 20% of total IoT applications, only marginally behind smart city ventures at 29% [2]. Despite these advances, IoT systems are contending with challenges such as latency (27%), power consumption (18%), and system dependability (14%) [2].

Healthcare and Blockchain: The healthcare sector, in particular, grapples with inefficiencies in patient data handling and emergency response mechanisms [3], [4]. This has prompted an increased focus on blockchain technology as a strategic solution for healthcare operational improvements [5]. With its decentralized, secure ledger infrastructure, blockchain is aptly positioned to address these issues, offering a patient-oriented model for health record management [6]. Such an approach grants patients greater control over their medical records, enhancing trust and collaborative interaction within healthcare frameworks [7].

Blockchain-Enhanced IoHT System: This paper introduces the full version of our previous work [8]. This innovative system merges blockchain with IoT, forming a blockchain-centric, patient-focused healthcare framework that incorporates smart contracts for efficient data governance. This solution addresses the shortcomings of existing IoT models by offering a secure, dependable, and efficient approach to healthcare data management.

Our designed platform utilizes blockchain for reliable and verifiable patient data recording. It features a brokerless and microservice architecture, guaranteeing resilience, scalability, and uninterrupted operation. The platform employs Role-based Access Control (RBAC) combined with a hierarchical approach to user management, allowing for comprehensive oversight of platform constituents like users and devices.

Incorporating blockchain, the platform facilitates secure and trustworthy data exchanges, overcoming key challenges inherent in traditional healthcare systems. Smart contracts are employed to streamline healthcare data management, thereby elevating the system's operational efficiency and reliability. This research makes significant contributions in several areas:

- Developing a patient-centered framework using microservice and brokerless architecture to improve system resilience, scalability, and availability.
- Implementing blockchain for enhanced transparency in data storage, enabling secure and trackable data exchange.
- Utilizing smart contracts to reinforce security, particularly in interactions between patients and service

providers, and to automate data management processes.

- Demonstrating a practical application of our model, showcasing its relevance and transformative potential in healthcare data management.
- Conducting a thorough evaluation of the system's architecture and blockchain integration, underlining its advantages over conventional healthcare data management methods.

Organization of the Paper: The remainder of this paper is organized as follows: Section II provides a review of the current state of healthcare data management systems and the role of blockchain in this context. Section III delves into the details of our Blockchain-Enhanced IoHT model, discussing its architecture, implementation, patient-centric focus, and the integration of blockchain technology and smart contracts. Following this, Section IV presents an assessment of our system, examining its performance and effectiveness. Finally, Section V concludes the paper, summarizing our key observations and exploring potential future research avenues.

II. Related Work

A. IoT Architectural Models in Healthcare

Diverse architectural solutions for gathering data from medical devices have been explored in literature. Maktoubian et al. [9] put forth an architecture that amalgamates MQTT protocol with Kafka Message Queue. Despite Kafka ensuring secure data transfer, MQTT protocol and its brokering structure encounter issues like possible single point failures and ambiguous Quality-of-Service (QoS) levels [10], [11]. Their system's security protocols remain largely unaddressed.

Another approach by Taher et al. [12] describes an IoT-cloud system aimed at medical data assimilation and processing. Although comprehensive, it depends on the MQTT protocol, which is hampered by security concerns [13]. Partha Pratim Ray [14] introduced a system for medical data collection using web socket and HTTP, yet these protocols have high memory demands and are not optimal for low-end devices [15].

Ha Xuan Son et al. [16] developed a patient emergency system employing blockchain on Hyperledger Fabric, with a focus on access control. However, the data collection method from patients and the system's scalability aspects were not elaborated upon.

B. Microservice and Brokerless Architecture in IoHT

Jita et al. [17] developed a home-based medical care system using a scalable microservice architecture, enhanced with blockchain security. The system, however, is based on the Zetta IoT Platform, utilizing HTTP and RESTful protocols, which are less efficient for low-end devices [15]. While other studies [18], [19] acknowledge the significance of microservices in healthcare, they fall short in practical implementation details.

Di Zeng et al. [20] introduced a medical system model that combines microservice with a brokerless structure, but it remains unimplemented. Similarly, Lam et al. [21], [22], [23] illustrated architectures incorporating MQTT broker, Single Sign-On, and Kafka message queue, achieving a compromise between transmission efficiency, reliability, and security.

C. Blockchain Implementation in Healthcare Systems

Blockchain technology has been incorporated into healthcare systems with varying focal points. Son et al. [3] and Le et al. [4] devised blockchain-based frameworks for access control in emergencies, prioritizing patient data confidentiality.

Le et al. [5] devised a blockchain system for medical waste management, underlining the need for secure information sharing about medical equipment and supplies, especially pertinent during the COVID-19 crisis. In another study, Le et al. [24] proposed a blockchain system for blood donation networks, tackling blood quality, supply, and distribution challenges.

Quynh et al. [25] suggested a blockchain system for managing national blood donation networks, streamlining blood supply and demand. Duong et al. [6], [7] proposed patient-focused healthcare systems utilizing blockchain smart contracts, emphasizing patient access, traceability, and control over health records.

These studies underscore the efficacy of blockchain in bolstering data security, privacy, and patient-centric approaches in healthcare. Our research builds upon these foundations, introducing a blockchain-enhanced IoHT platform that combines microservice and brokerless architecture to augment scalability, efficiency, and control over patient data.

III. System Architecture

A. Architectural Overview of Blockchain-Enhanced IoHT-MBA Platform

The proposed blockchain-enhanced IoHT-MBA platform is based on a layered architecture, incorporating the edge layer, blockchain layer, and cloud layer.

1) Edge Layer: The edge layer includes local devices of the patient like smartphones, sensors, and other IoT devices, functioning as the primary data collectors and processors. Each of these devices is integrated with a simplified blockchain client, facilitating communication with the blockchain layer. Data retention on these devices is localized, bolstering both privacy and security.

2) Blockchain Layer: At the heart of our patient-centric data management system lies the blockchain layer. Leveraging Hyperledger Fabric, a permissioned blockchain framework, we establish a secure, transparent ecosystem for data handling. Here, only synthesized health data and related transactions are stored. The validation and recording of transactions across various nodes reinforce data integrity and traceability. Smart contracts, or chaincodes in Hyperledger Fabric, automate agreement execution pertaining to data sharing. These contracts encode patient privacy conditions, executing upon data access or sharing requests to ensure compliance with patient preferences.

3) Cloud Layer: The cloud layer offers diverse services like data analytics and health monitoring to platform users. It interfaces with the blockchain layer for data access, adhering to privacy terms defined in smart contracts and accessing only aggregated blockchain data.

This structure of the platform ensures a secure, decentralized, and patient-focused data management approach in healthcare IoT. Subsequent sections will elaborate on the platform's implementation and evaluation.

B. Detailed Architecture

The system's design incorporates microservices and brokerless architecture, enhancing fault tolerance, scalability, and operational efficiency. Microservices architecture refers to developing applications as a collection of small, autonomous services, each operating in its own environment and communicating through lightweight mechanisms like HTTP/REST with JSON or Protobuf. In our case, gRPC is employed for enhanced speed[1]. This architecture allows for independent updating, deployment, and scaling of individual services. The brokerless architecture removes the necessity for a central broker or server, thus eliminating single points of failure and enhancing scalability. It allows direct communication among nodes or devices, crucial for reliability and efficiency in healthcare settings.

The combination of these architectures equips our system to efficiently manage a vast array of devices and data while maintaining high availability and performance. Further sections will detail the patient-side data consumption in edge computing (refer to Fig. 1) and the overall architecture of the Blockchain-Enhanced IoHT platform (refer to Fig. 2).

1) Edge Computing Architecture: The edge computing component encompasses two primary layers: the Things layer and the Client layer (see Fig. 1).

a) Things Layer: This layer consists of various medical devices owned by the patient, like wearables and IoT medical devices. Each device is outfitted with sensors to gather crucial health data. These devices manage two independent services: data collection and control services. Data collection involves continuous monitoring and streaming to edge computing services, with patient authentication and authorization checks for data security. The control service enables remote adjustments to the devices, catering to specific health needs and preferences.

b) Client Layer: The Client layer, represented by patients, allows device management and data monitoring. Patients control their health data, managing sharing permissions and ensuring their privacy preferences are upheld. This layer's centrality to the architecture underlines the patient-centric nature of data management in our platform.

Edge computing in our platform processes data near its source, minimizing latency and enhancing real-time processing. Patient control over devices and data underscores the platform's focus on patient autonomy and privacy.

2) Blockchain-Enhanced IoHT Architecture: Fig. 2 depicts the Blockchain-Enhanced IoHT platform architecture, enabling secure and efficient data transmission from medical devices to the distributed ledger and service providers.

a) Data Processing Services: Post-collection at the edge, health data undergoes further processing in data processing services. Tasks include data cleaning, transformation, and feature extraction. Aggregated data, instead of raw patient data, is stored in the blockchain for enhanced efficiency and privacy.

b) Distributed Ledger and Smart Contracts: Aggregated data is stored in the distributed ledger, validated by multiple nodes for integrity. Smart contracts in our system serve two functions:

- Data Access Control: Smart contracts contain metadata parameters reflecting patient privacy preferences. Service provider access requests are checked against these parameters, ensuring compliance with patient privacy conditions.
- Data Usage Control: They also regulate how service providers can use the data, adhering to conditions set within the contract.

c) Service Providers: Service providers, including healthcare professionals and researchers, access ledger-stored data. Their access is contingent on meeting the privacy conditions set in the smart contracts.

The Blockchain-Enhanced IoHT platform thus ensures patient control over their data, while facilitating secure and transparent data sharing with service providers.

IV. Evaluation Scenarios

A. Evaluating Performance Using Microservice and Brokerless Architectural Approach

1) Configuration of the Test Environment: Our innovative Blockchain-Enhanced IoHT system utilizes a microservice architecture for optimal performance. During our evaluation phase, the services of this platform were hosted on the Amazon EC2 platform[2]. We configured each service to mirror a virtual machine setup, equipped with 1GB of RAM and a single vCPU for realistic testing conditions. Additionally, client-side services, including data collection and control, were implemented on the Raspberry Pi 3 model B+ modules[3]. These modules are powered by the Broadcom BCM2837, an ARMv8 (64bit) quad-core processor clocking at 1.2 GHz, and are also furnished with 1GB RAM, providing a robust environment for our system's deployment and testing.

2) Evaluation of Round Trip Time: In gauging the efficacy of data transmission within the system, the Round Trip Time (RTT) is employed, measured from the instance data is transmitted from IoT devices until it reaches the Message Queue. Alongside this, an examination of the error rate, quantified as the ratio of lost messages to the total, is conducted. For a thorough assessment, instances of EC2 VMs equivalent to the Rasberry Pi model B + module are generated in diverse geographical locations. These locations encompass North California, Stockholm, Ho Chi Minh City, and Sydney.

[1] For detailed implementation, see our prior work [26], [27]

[2] https://aws.amazon.com/

[3] https://www.raspberrypi.org/products/raspberry-pi-3-model-b/

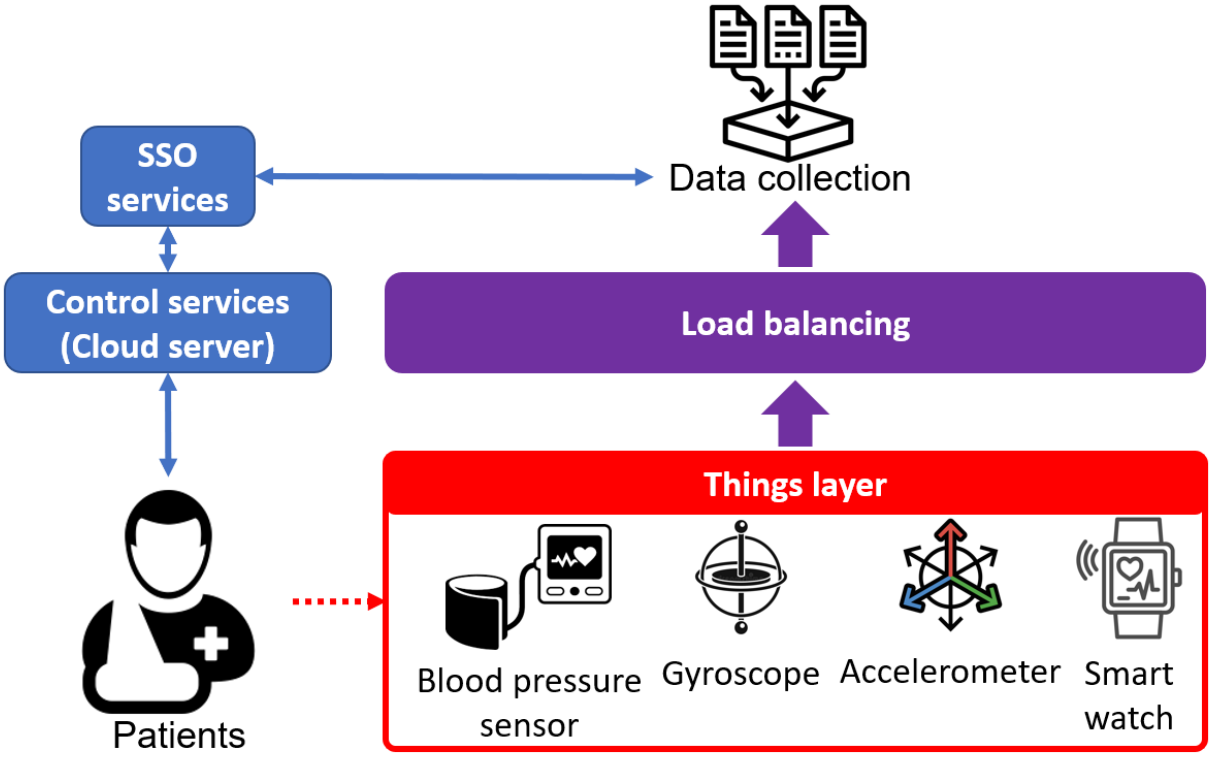

Fig. 1. Patient-side edge computing based on microservice and brokerless architecture.

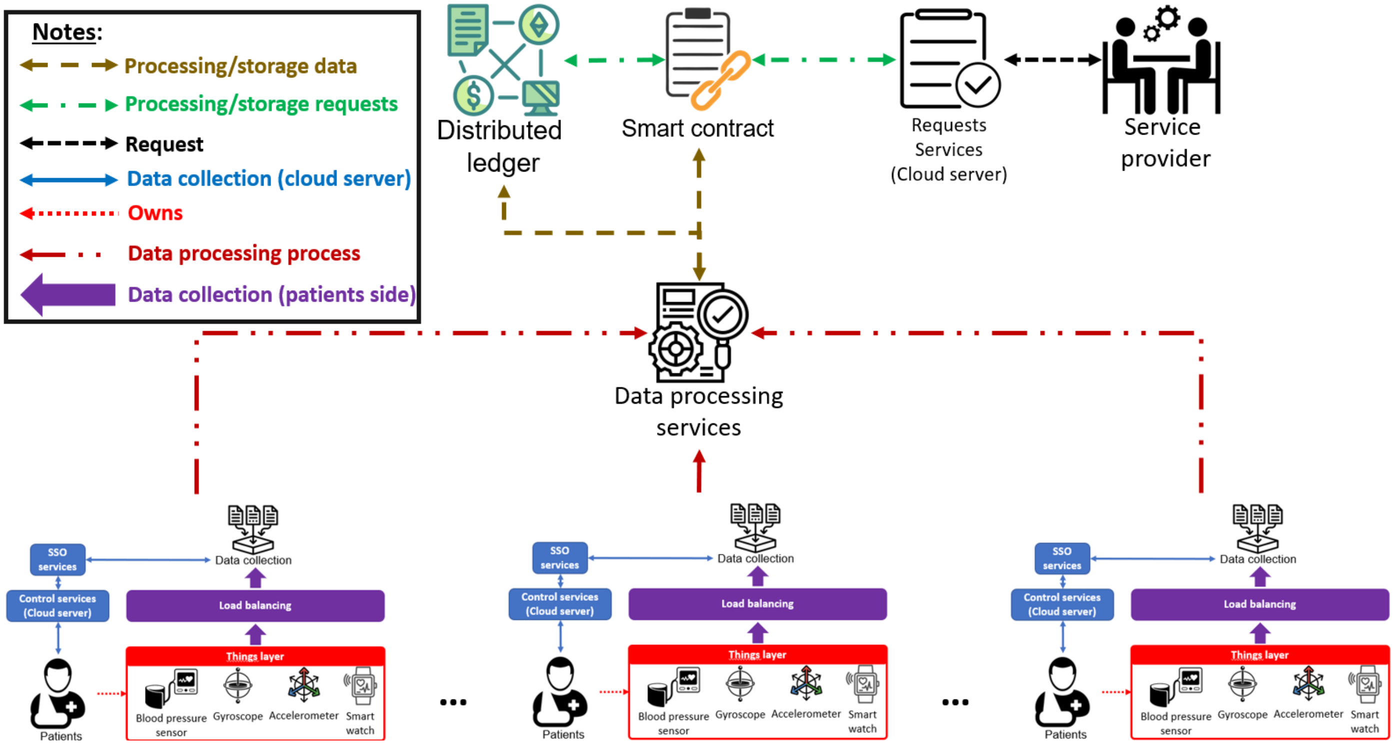

Fig. 2. Blockchain-Enhanced IoHT platform architecture.

The objective is to analyze the impact of location on both delay time and error rate during the streaming of data. The findings from these evaluations are succinctly summarized in Table I.

Table I illustrates the Round Trip Time (RTT) and error rates associated with data communication in the Blockchain-Enhanced Internet of Health Things (IoHT) platform, observed across diverse geographical locations: North California, Stockholm, Ho Chi Minh City, and Sydney. The RTT is examined for varying message volumes: 1,000; 5,000; 10,000; 50,000; and 100,000.

The RTT, in this context, measures the time taken for a message to travel from an IoT device (sender) to the Message Queue (receiver) and back.

The table provides the following insights:

- In North California, RTT ranges from 3.23 seconds for 1,000 messages to 259.11 seconds for 100,000 messages, with a consistent 0% error rate across all message volumes.
- In Stockholm, RTT varies from 3.41 seconds for 1,000 messages to 259.43 seconds for 100,000 messages, maintaining a 0% error rate for all message volumes.
- In Ho Chi Minh City, RTT spans from 3.62 seconds for 1,000 messages to 259.98 seconds for 100,000 messages, accompanied by a 0% error rate across all message volumes.
- In Sydney, RTT ranges from 3.21 seconds for 1,000 messages to 258.06 seconds for 100,000 messages, with a consistent 0% error rate for all message volumes.

The error rate represents the proportion of lost messages during transmission. A 0% error rate across locations and message volumes indicates flawless transmission without any losses.

This table underscores the Blockchain-Enhanced IoHT platform's robust performance across varied geographical locations and message volumes. Despite increasing message volumes, the RTT exhibits linear growth, and the platform demonstrates resilience by maintaining a 0% error rate, affirming its reliability.

3) Robustness Against Connection Failures: Evaluating the performance of the Blockchain-Enhanced Internet of Health Things (IoHT) platform under connection failures is vital, especially in healthcare applications where data integrity and reliability are paramount. Disruptions in data transmission can potentially lead to incorrect diagnoses or interventions, significantly impacting patient care.

To gauge the system's resilience in the face of connection failures, we conducted simulations of broken connections between the data publisher (i.e., the healthcare IoT device) and the subscriber (i.e., the data processing or storage service). We then compared the number of messages received by the subscriber in scenarios with and without the utilization of the Blockchain-Enhanced IoHT platform.

As illustrated in Fig. 3, in the absence of our platform, the subscriber only captures the latest message sent by the publisher when a connection failure occurs. This limitation arises from the retain function of the MQTT protocol[4] which retains only the most recent message, resulting in the loss of any data published during the disconnection period.

Conversely, when employing the Blockchain-Enhanced IoHT platform, the subscriber receives all messages published by the sender, including those transmitted during the connection failure. This capability is facilitated by the Kafka message queue, which preserves all outgoing messages until successful delivery, thereby preventing any data loss during transmission.

The capacity to recover and process all data following a connection failure is a critical attribute for a healthcare IoT system. It ensures the reliable reception of all patient data irrespective of network conditions, preserving the integrity of medical data and facilitating accurate and comprehensive analysis for improved patient care outcomes.

B. Evaluation of Performance using Hyperledger Fabric

To comprehensively gauge the efficacy of our proposed Blockchain-Enhanced Internet of Health Things (IoHT) model, an in-depth performance analysis was carried out utilizing Hyperledger Caliper, a benchmarking tool tailored for blockchain systems. The focal performance indicators included the count of successful and unsuccessful requests, transaction rate (Send Rate in transactions per second, or TPS), latency (maximum, minimum, and average, in seconds), and throughput (TPS).

Our assessment encompassed five distinct scenarios, each representing varying loads on the system (ranging from 1,000 to 5,000 requests per second). The evaluation ceased at 5,000 requests per second, as we observed a notable surge in the number of failed requests beyond this threshold, particularly in scenarios involving data updates.

1) Medical Data Creation Performance: Table II delineates the performance metrics for medical data creation under diverse loads. Notably, the count of successful requests oscillates between 27,000 and 31,000, while failed requests range from 16,000 to 19,000. Interestingly, the correlation between the number of successful and failed requests and the system load appears inconclusive, underscoring the robustness of our platform. The transaction rate remains consistent across all scenarios, hovering between 135 and 150 transactions per second (TPS).

Regarding latency, the maximum latency spans from approximately 1,457 seconds (for 3,000 requests per second) to around 1,712 seconds (for 5,000 requests per second). Minimum latency varies from under 1 second (for 1,000 requests per second) to approximately 12 seconds (for 3,000 requests per second). The average latency fluctuates between 650 and 700 seconds per request, contingent on the system load. Meanwhile, throughput maintains steady performance within the range of 12 to 17 TPS.

2) Performance Evaluation of Medical Data Queries: To assess the system's performance under varying data query loads, we conducted tests across five scenarios, ranging from 1,000 to 5,000 data retrieval requests per second. As depicted in Table III, the count of successful requests consistently

[4] For further details, we refer the reader to our prior publications [28], [27]

TABLE I. ROUND TRIP TIME RESULTS IN THE FOUR PLACES

Location	Factor	1,000	5,000	10,000	50,000	100,000
North California	RTT(s)	3.23	13.78	27.42	131.16	259.11
	Error(%)	0	0	0	0	0
Stockholm	RTT(s)	3.41	13.98	25.86	129.14	259.43
	Error(%)	0	0	0	0	0
Ho Chi Minh city	RTT(s)	3.62	13.74	24.93	131.11	259.98
	Error(%)	0	0	0	0	0
Sydney	RTT(s)	3.21	14.02	26.08	129.98	258.06
	Error(%)	0	0	0	0	0

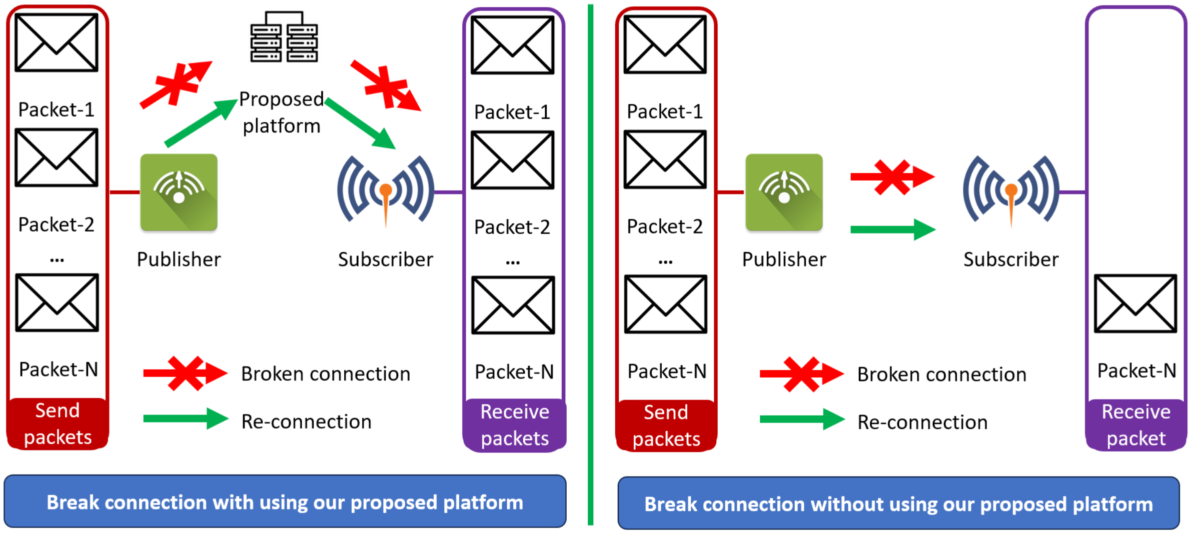

Fig. 3. Number of received messages when the system recovers after a broken connection issue.

TABLE II. MEDICAL DATA CREATION PERFORMANCE IN FIVE INCREASING EACH 1,000 REQUESTS SCENARIOS

Name	Success	Fail	Send Rate (TPS)	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Throughput (TPS)
1,000 request	26,987	19,801	135.0	1,532.18	10.41	654.12	11.9
2,000 request	29,604	16,402	138.5	1,523.78	9.82	634.21	16.4
3,000 request	27,412	18,523	142.7	1,457.34	10.43	678.43	15.3
4,000 request	29,617	19,176	139.9	1,686.23	10.67	651.24	15.4
5,000 request	30,401	16,205	145.6	1,712.12	11.01	696.18	17.2

surpasses 106,000, with failed requests remaining below 5,000. This noteworthy outcome underscores the system's capability to effectively retrieve a substantial volume of medical data under significant loads. Analogous to the data creation scenario, both the Send Rate (TPS) and Throughput (TPS) exhibit stability, experiencing minor fluctuations around 325 to 360 and approximately 290, respectively.

Concerning system latency, maximum latency remains approximately 250 seconds across all five measurement scenarios. The minimum latency is virtually negligible, at about 0.01 seconds. On average, each data query request receives a response within roughly 5 seconds. These outcomes illustrate the efficiency of our Blockchain-Enhanced IoHT platform in managing both data creation and retrieval requests, crucial operations in a patient-centric Internet of Healthcare Things system.

C. Discussion

The evaluation of our proposed Blockchain-Enhanced IoHT system yields valuable insights into its performance and efficiency. The system's brokerless and microservice architecture, coupled with a blockchain-based data management approach, showcases its potential to handle a substantial number of data transactions while maintaining low latency and high throughput.

The system underwent testing under diverse load conditions, with request volumes ranging from 1,000 to 5,000 per second. Even under heightened loads, the system demonstrated resilience and stability, sustaining a consistent response time and minimal error rates. The brokerless architecture, employing the gRPC protocol, exhibited notable improvements in CPU and RAM usage compared to other IoHT protocols, indicative of efficient resource utilization.

TABLE III. MEDICAL DATA QUERY PERFORMANCE IN FIVE INCREASING EACH 1,000 REQUESTS SCENARIOS

Name	Success	Fail	Send Rate (TPS)	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Throughput (TPS)
1,000 request	103,321	4,232	356.0	254.14	0.01	4.89	289.18
2,000 request	108,208	4,456	323.5	256.23	0.01	5.08	298.45
3,000 request	103,661	4,281	345.8	252.51	0.01	4.23	294.01
4,000 request	108,129	4,928	341.4	250.65	0.01	4.83	293.21
5,000 request	106,224	3,265	323.9	256.12	0.01	5.01	298.11

V. DISCUSSION

A. Remarkable Insights

As we delve into the intricacies of gas metrics across various blockchain platforms, a plethora of distinct patterns and insights emerge, which hold significant relevance for both blockchain developers and users alike.

1) Uniformity vs. Variability: One of the notable observations is the trade-off between uniformity and variability in gas pricing. The BNB Smart Chain stands out for its uniformity, maintaining a consistent gas price of 0.00000001 BNB (equivalent to 10 Gwei) across all actions. This predictability can be advantageous for users as it ensures a constant expectation of costs. In contrast, platforms like Polygon introduce minor discrepancies in gas prices across different operations. While these variations might seem subtle, they can accumulate substantial costs in high-frequency actions, making it a critical consideration for blockchain investors and developers.

2) Cost-Efficiency: Fantom's gas pricing strategy is particularly noteworthy, with a remarkably lower gas price of 3.5 Gwei compared to BNB Smart Chain's 10 Gwei. This significant difference can translate into considerable cost savings for users engaged in large transaction volumes. It underscores the importance of gas pricing as a pivotal factor influencing the economic feasibility of utilizing a particular blockchain platform.

3) Complexity in Pricing: Polygon's nuanced gas pricing structure may arise from its inherent design or a deliberate effort to fine-tune pricing for specific operations. While this complexity might introduce challenges for the average user, it offers enhanced flexibility for businesses and developers. The ability to tailor gas costs for different operations can be advantageous for optimizing resource allocation in specific use cases.

4) Operational Capacity and Efficiency: Efficiency in gas consumption during operations is another critical aspect to consider. For instance, Celo demonstrates that it utilizes only 76.92

5) Strategic Implications for Projects: The insights gained from this analysis have strategic implications for blockchain projects, especially startups and new ventures. Beyond just the direct costs, factors such as operational efficiency, pricing flexibility, and predictability play a crucial role in platform selection. These considerations can significantly influence decisions regarding project launches, investments, and day-to-day transactions.

6) User Considerations: For the average user, clarity and predictability in transaction costs are paramount. Platforms with transparent and straightforward pricing models may be more attractive. On the other hand, platforms that offer flexibility in pricing and demonstrate optimal resource consumption may be favored by traders, businesses, and advanced users seeking to fine-tune their operations.

B. Future Directions

In the subsequent phases of our research, we are eager to delve even deeper into the intricacies of transaction costs and gas metrics. This will involve the integration of advanced methodologies and intricate data structures. Specifically, we plan to implement sophisticated encryption-decryption techniques to provide a clearer and more detailed picture of transaction overheads [29]. Taking our proposed model from theoretical analysis to practical application is another exciting avenue of exploration. We intend to execute the recommendation system over the Fantom (FTM) mainnet to validate its performance in real-world scenarios. This real-world validation will help us refine our model and make it more robust.

Furthermore, our current analysis has not explored the nuances of user privacy policies, which are of paramount importance in today's digital transactions [30], [31]. Building upon established research in access control and dynamic policy models, we envision enhancing our system's capabilities to address these privacy concerns comprehensively [16].

From an infrastructural standpoint, we are considering the integration of modern techniques and paradigms such as gRPC, Microservices, dynamic messaging paradigms, and brokerless models [26], [21]. These integrations will not only augment the robustness of our framework but also enhance user interactions, particularly in terms of API-driven communication [23]. This forward-looking approach will ensure that our research remains at the forefront of blockchain technology advancements [22], [27].

VI. CONCLUSION

In this research, we introduced a cutting-edge, patient-centric framework known as the Blockchain-Enhanced IoHT. This innovative system integrates a microservice and brokerless architecture, significantly enhancing its fault tolerance, scalability, and overall availability. Such an architecture not only fortifies the system's robustness but also renders healthcare data management more efficient and resilient. The incorporation of blockchain technology into the system guarantees secure and easily traceable data sharing, effectively tackling the prevalent challenges faced in traditional healthcare systems. Moreover, the employment of smart contracts in this model reinforces security, especially in managing the interactions between patients and healthcare providers, thus boosting the system's efficiency and dependability. The proof-of-concept showcased within this study validates the practicality and potential of our proposed model in revolutionizing healthcare data management. Our evaluation of the Blockchain-Enhanced

IoHT, focusing on its architectural design and blockchain integration, sheds light on its capabilities in managing healthcare data efficiently.

Looking ahead, our future endeavors will concentrate on refining the system's performance further. This includes exploring avenues to amplify the scalability and efficiency of the blockchain component and delving into the integration of more sophisticated security measures. Our ultimate goal is to propel advancements in the realm of healthcare data management, aiming to substantially improve patient care and outcomes.

References

[1] F. Dahlqvist *et al.*, "Growing opportunities in the internet of things," *McKinsey, July*, 2019.

[2] P. Asghari *et al.*, "Internet of things applications: A systematic review," *Computer Networks*, vol. 148, pp. 241–261, 2019.

[3] H. X. Son *et al.*, "Toward a blockchain-based technology in dealing with emergencies in patient-centered healthcare systems," in *Mobile, Secure, and Programmable Networking: 6th International Conference, MSPN 2020, Paris, France, October 28–29, 2020, Revised Selected Papers 6*. Springer, 2021, pp. 44–56.

[4] H. T. Le *et al.*, "Patient-chain: patient-centered healthcare system a blockchain-based technology in dealing with emergencies," in *International Conference on Parallel and Distributed Computing: Applications and Technologies*. Springer, 2021, pp. 576–583.

[5] ——, "Medical-waste chain: a medical waste collection, classification and treatment management by blockchain technology," *Computers*, vol. 11, no. 7, p. 113, 2022.

[6] N. Duong-Trung *et al.*, "Smart care: integrating blockchain technology into the design of patient-centered healthcare systems," in *Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy*, 2020, pp. 105–109.

[7] ——, "On components of a patient-centered healthcare system using smart contract," in *Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy*, 2020, pp. 31–35.

[8] T. Nam *et al.*, "Spamer: Securing patient medical records in the cloud-a microservice and brokerless architecture approach," in *International Conference on Web Services*. Springer, 2023, pp. 32–46.

[9] J. Maktoubian and K. Ansari, "An iot architecture for preventive maintenance of medical devices in healthcare organizations," *Health and Technology*, vol. 9, no. 3, pp. 233–243, 2019.

[10] M. B. Yassein, M. Q. Shatnawi, S. Aljwarneh, and R. Al-Hatmi, "Internet of things: Survey and open issues of mqtt protocol," in *2017 international conference on engineering & MIS (ICEMIS)*. IEEE, 2017, pp. 1–6.

[11] J. Toldinas, B. Lozinskis, E. Baranauskas, and A. Dobrovolskis, "Mqtt quality of service versus energy consumption," in *2019 23rd International Conference Electronics*. IEEE, 2019, pp. 1–4.

[12] N. C. Taher, I. Mallat, N. Agoulmine, and N. El-Mawass, "An iot-cloud based solution for real-time and batch processing of big data: Application in healthcare," in *2019 3rd International Conference on Bio-engineering for Smart Technologies (BioSMART)*. IEEE, 2019, pp. 1–8.

[13] J. J. Anthraper and J. Kotak, "Security, privacy and forensic concern of mqtt protocol," in *Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India*, 2019.

[14] P. Pratim Ray, D. Dash, and N. Moustafa, "Streaming service provisioning in iot-based healthcare: An integrated edge-cloud perspective," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 11, p. e4109, 2020.

[15] M. Bansal *et al.*, "Application layer protocols for internet of healthcare things (ioht)," in *2020 Fourth International Conference on Inventive Systems and Control (ICISC)*. IEEE, 2020, pp. 369–376.

[16] H. X. Son *et al.*, "Toward an privacy protection based on access control model in hybrid cloud for healthcare systems," in *International Joint Conference: 12th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2019)*. Springer, 2020, pp. 77–86.

[17] H. Jita and V. Pieterse, "A framework to apply the internet of things for medical care in a home environment," in *Proceedings of the 2018 International Conference on Cloud Computing and Internet of Things*, 2018, pp. 45–54.

[18] R. Hill, D. Shadija, and M. Rezai, "Enabling community health care with microservices," in *2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on Ubiquitous Computing and Communications (ISPA/IUCC)*. IEEE, 2017, pp. 1444–1450.

[19] H. X. Son *et al.*, "Towards a mechanism for protecting seller's interest of cash on delivery by using smart contract in hyperledger," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 4, 2019.

[20] D. Zheng, X. Zhang, and L. Chen, "Research of new integrated medical and health clouding system based on configurable microservice architecture," in *2020 IEEE 23rd International Conference on Computational Science and Engineering (CSE)*. IEEE, 2020, pp. 78–85.

[21] T. T. L. Nguyen *et al.*, "Toward a unique iot network via single sign-on protocol and message queue," in *Computer Information Systems and Industrial Management: 20th International Conference*. Springer, 2021, pp. 270–284.

[22] L. N. T. Thanh *et al.*, "Toward a security iot platform with high rate transmission and low energy consumption," in *Computational Science and Its Applications–ICCSA 2021: 21st International Conference*. Springer, 2021, pp. 647–662.

[23] ——, "Uip2sop: a unique iot network applying single sign-on and message queue protocol," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 6, 2021.

[24] H. T. Le *et al.*, "Bloodchain: a blood donation network managed by blockchain technologies," *Network*, vol. 2, no. 1, pp. 21–35, 2022.

[25] N. T. T. Quynh *et al.*, "Toward a design of blood donation management by blockchain technologies," in *Computational Science and Its Applications–ICCSA 2021: 21st International Conference*. Springer, 2021, pp. 78–90.

[26] L. T. T. Nguyen *et al.*, "Bmdd: a novel approach for iot platform (broker-less and microservice architecture, decentralized identity, and dynamic transmission messages)," *PeerJ Computer Science*, vol. 8, p. e950, 2022.

[27] L. N. T. Thanh *et al.*, "Sip-mba: a secure iot platform with brokerless and micro-service architecture," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 7, 2021.

[28] ——, "Ioht-mba: an internet of healthcare things (ioht) platform based on microservice and brokerless architecture," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 7, 2021.

[29] K. L. Quoc *et al.*, "Sssb: An approach to insurance for cross-border exchange by using smart contracts," in *Mobile Web and Intelligent Information Systems: 18th International Conference*. Springer, 2022, pp. 179–192.

[30] H. X. Son and N. M. Hoang, "A novel attribute-based access control system for fine-grained privacy protection," in *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*, 2019, pp. 76–80.

[31] N. M. Hoang and H. X. Son, "A dynamic solution for fine-grained policy conflict resolution," in *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*, 2019, pp. 116–120.