A Novel IoT Middleware for Secure Pharmaceuticals Condition Monitoring in Supply Chain

ISHMILH, Osama, JARWAR, Aslam <http://orcid.org/0000-0002-5332-1698> and JAVED, Yasir

A Novel IoT Middleware for Secure Pharmaceuticals Condition Monitoring in Supply Chain

Osama Ishmilh*†, Muhammad Aslam Jarwar†, Yasir Javed†

*Department of Programming, Economic Information Centre, Tripoli, Libya

†Department of Computing, Sheffield Hallam University, Sheffield, United Kingdom

osama.ishmilh@student.shu.ac.uk, osama.ishmilh@eidc.gov.ly, a.jarwar@shu.ac.uk, y.javed@shu.ac.uk

***Abstract*—This paper explores the potential of blockchain technology and the Internet of Things (IoT) to enhance safety and traceability for the pharmaceutical supply chain, primarily focusing on medication storage. This research arises from challenges tied to improper warehousing procedures and the requirement for flawless data accuracy among various participants in the supply chain. In order to track and monitor the conditions of medical supplies, an IoT middleware is developed that utilises the Hyperledger Fabric Blockchain. The data gathered from IoT end-points is securely transmitted to the node running the HyperLedger Blockchain using the MQTT protocol. The developed prototype provides an immutable history of drug storage conditions, such as temperature, and humidity. To ascertain the system's performance, we have conducted systematic tests. The experimental results suggest that the developed proof of concept demonstrates its ability to handle different loads, maintain optimal transaction throughput and latency and efficiently manage and secure IoT data in real-time. Moreover, it ensures continuous data collection from supply chain IoT nodes and synchronisation with the blockchain network.**

I. Introduction

Ensuring optimal storage conditions for pharmaceutical products is critical in preserving their quality, efficacy, and safety. Effective storage practices help prevent issues such as degradation, contamination, or damage. As a result, this facilitates the provision of reliable and effective medications, thereby enhancing patient safety and improving health outcomes [10].

However, tracing the history of drug storage conditions throughout the supply chain poses considerable challenges. Inadequate monitoring and recording of crucial information, for instance, temperature and humidity, could compromise medication integrity, leading to risks of distributing medications with uncertain efficacy and furthermore, could result in ineffective treatment of patients' medical conditions. In the worst case, degraded medications may induce unexpected side effects or produce harmful by-products, which may harm patients' health [4]. Nokhodchi and Javadzadeh [9] stated that tablets could go through chemical changes and lose their effectiveness if they are stored in temperatures, humidity levels, and moisture conditions that are not suitable.

To resolve these challenges, the requirement for secure and transparent systems for managing pharmaceutical warehousing data is proposed. Such systems should leverage technology to provide real-time updates and ensure data security and accuracy. Considering these aspects, the primary aim of this paper is to enhance the understanding of effective strategies to maintain the integrity of pharmaceuticals during the storage stage of the supply chain. In particular, the study delves into the promising yet underexplored area of integrating blockchain and IoT technologies, viewing them as potential approaches to improve traceability and preserve drug quality.

Blockchain could record a transparent and immutable log of medicine storage conditions, whereas IoT devices like temperature and humidity sensors can continuously monitor and report in real time. The data collected can provide valuable insights into the environmental factors affecting the quality and integrity of medications from storage facilities. Integration of these technologies can substantially improve traceability and guarantee the safety of pharmaceutical products throughout the supply chain [11].

Consequently, this paper aims to propose a blockchain-based IoT middleware to address the aforementioned challenges. This proposed solution has the potential to enhance patient safety and improve public health digital services. To achieve these aims and objectives, this research seeks to answer the following question:

How can blockchain be integrated with Internet of Things technologies to develop a secure system for monitoring and tracking the conditions of pharmaceutical items in the supply chain?

In line with the aims, and objectives, this paper makes the following contributions:

- To develop a blockchain-based IoT middleware to monitor and record the pharmaceutical product's supply chain.
- Assess interoperability as a component of advanced IoT middleware for secure data representation and sharing, and develop an interoperable scheme.
- Finally, develop test scenarios for the IoT middleware developed, analyse the results of these tests, evaluate the

system's effectiveness, and identify potential areas for future research and improvement.

The remainder of this paper is structured as follows. Section II reviews related work focusing on applied blockchain research and IoT technologies, and their efficacy in healthcare. Section III presents the conceptual model of the proposed middleware. Section IV describes the system design and implementation setup. Sections V and VI discuss the performance analysis and evaluation. Finally, the conclusion of the study is provided in Section VII.

II. Related Work

A. Blockchain in Healthcare

Blockchain technology is extensively explored in healthcare, serving various purposes like managing patient records, securing pharmaceutical supply chains, facilitating insurance claims, and enabling medical research [2], [13].

Durneva, Cousins, and Chen (2020) [3] systematically reviewed blockchain applications in patient care. Findings revealed its use in critical areas including electronic health records, personal health records, health information exchanges, and clinical trials aiming to address security, privacy, interoperability, and health outcomes challenges. However, notable barriers persist, like legacy system integration, storage limitations, and adoption resistance. Durneva, Cousins, and Chen (2020) also suggested future research directions including improving compatibility, addressing storage constraints, promoting adoption, and exploring disruptive applications. In summary, while blockchain holds healthcare transformation potential, many applications remain conceptual.

Xie et al. (2021) [13] reviewed current and projected healthcare blockchain applications. The distributed ledger system offers secure, cross-institutional health data management. Use cases include preserving electronic records, enabling data sharing across institutions, streamlining insurance claims, securing medicine supply chains, preventing e-prescription fraud, and validating competencies in medical education and research. Furthermore, blockchain shows promise supporting public health initiatives like pandemic response tracking.

B. Internet of Things in Healthcare

The Internet of Things (IoT) is transforming healthcare by enabling connected networks of medical devices and systems to improve patient monitoring, care coordination, and operational efficiency. Numerous studies have reviewed IoT applications in healthcare [1], [5], [6], [12].

Islam et al. (2015) [5] provided an early overview of IoT in healthcare, highlighting potential benefits like remote patient monitoring, improved drug management, and medical device integration. However, they note obstacles to large-scale adoption including interoperability, security, and privacy concerns that must be addressed.

Uddin et al. (2019) [12] surveyed the state of IoT in healthcare. They summarize major application areas like chronic disease management, elderly care, and hospital workflow optimization. Key enabling technologies examined include wearable sensors, implanted devices, trackers, and ambient assisted living platforms. The authors also outline IoT healthcare implementation challenges involving power, security, interoperability, costs, and patient willingness to adopt connected devices.

C. Challenges in Medicine Storage

Zamani and Wembridge (2022) [14]evaluated an automated temperature monitoring system deployed in medicine and vaccine storage at a hospital network in Australia. Their findings underscore the system's efficiency, as it detected significantly higher temperature excursions than previous methods. Specifically, it identified 28,746 excursions in refrigerators and 8,966 in ambient locations. Notably, most refrigerator excursions were within the range of +2°C (98.4). The study concludes continuous automated monitoring enhances visibility of temperature non-compliance, guiding effective solutions, and should encompass freezers, ambient storage, and refrigerators. Proposed improvements include avoiding unreliable brands and developing national medicine storage guidelines. Overall, this underscores automated system value ensuring proper medicine and vaccine storage temperatures.

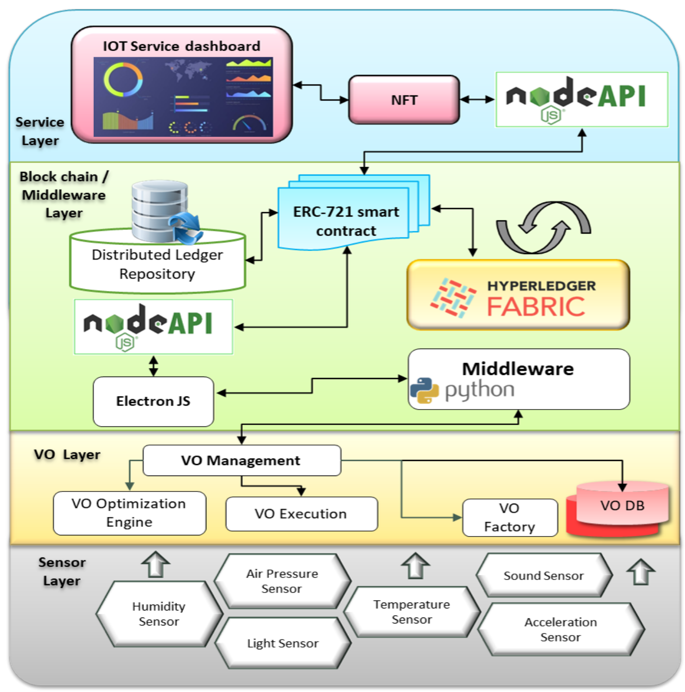

Fig. 1: Blockchain Hyperledger Fabric and IoT Integrated Middleware [7]

III. Proposed System

A. Conceptual Model of Middleware

Fig:1 illustrates the well-defined architecture of a Blockchain Hyperledger Fabric integrated with the IoT system. The proposed architecture, comprising several functional components at each level, ensures seamless integration and efficient operation [7]. The sensor layer collects data from

IoT devices at the edge. The virtualization layer semantically processes this data to support interoperability. The middleware layer facilitates data proliferation using technologies like MQTT and APIs. The blockchain layer employs a distributed ledger protocol to securely store digitalized sensor data and manage smart contracts. Lastly, the services layer provides user access via a mobile application dashboard, enabling secure control over data and sensor feeds from the distributed ledger.

B. High Level Components

The system follows a modular layered architecture for flexibility and separation of concerns. At the top is the application layer consisting of web applications. This allows users to interact with the system. The IoT layer collects real-time data from embedded sensors and devices. It provides connectivity to physical environments through standardized messaging protocols. Next is the integration layer with components like an API backend server in the middle. This layer handles seamless integration of the web applications with the core blockchain network and external systems like IoT devices. It stitches together the end-to-end workflow. At the bottom is the blockchain layer, which manages the distributed ledger, identities, smart contracts, consensus and other blockchain network functions. This provides the system with tamper-proof data sharing, provenance, and automation via decentralized logic. Fig:2 shows some high-level components at each layer.

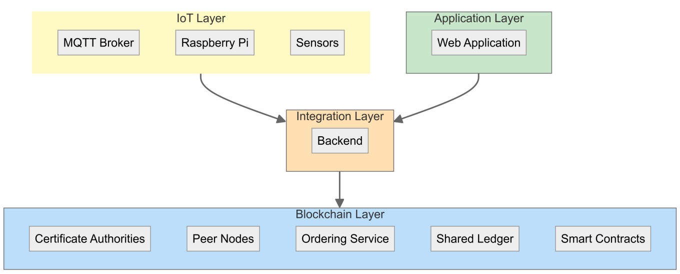

Fig. 2: Layer Wise High-Level Components

C. Implementation of The Proposed System

The proposed system employs a decentralized architecture integrating permissioned blockchain technology and IoT devices to enable trustworthy monitoring and tracking of medicine storage conditions throughout pharmaceutical supply chains. At the core is an immutable ledger maintained on a private Hyperledger Fabric blockchain network that securely records temperature and humidity data transmitted from IoT sensor devices in medicine storage environments. Raspberry Pi devices comprise the IoT layer, collecting real-time sensor measurements and transmitting them via secure channels to the integration middleware layer. This layer handles seamless data transfer between the IoT devices and blockchain network using lightweight protocols. Application programming interfaces enable querying the sensor data history from the blockchain ledger. This integrated system architecture provides transparent and verifiable visibility into storage conditions by combining the benefits of blockchain's permanence and provenance with the real-time granularity of IoT environmental data. The decentralized platform aims to bring accountability, integrity, and collaboration to pharmaceutical supply chain monitoring through crypto-secured data sharing and immutable records. A sample of two nodes exemplifies a complete blockchain configuration for each organization, establishing the blockchain network between them while retaining the capability to extend the network by adding nodes from other organizations in the future. Fig:3 illustrates the flow of proposed implementation.

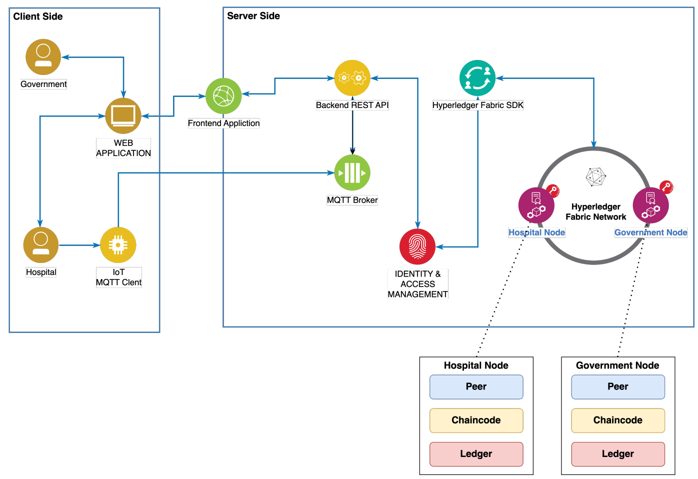

Fig. 3: Implementation Diagram of The Proposed System

Additionally, the sequence diagram in Fig:4 shows the end-to-end communication among the various components in proposed implementation:

- The IoT sensor continuously monitors the medicine storage environment and publishes the temperature and humidity data to the MQTT message broker topic.
- The Node.js backend application subscribes to the MQTT broker topic to receive any real-time sensor data messages.
- Upon receiving new sensor data, the backend application prepares a transaction proposal to submit to the Hyperledger Fabric network. This stores the sensor data on the immutable ledger.
- The Fabric network follows the endorsement policy, ordering, and validation process to commit the transaction and update the ledger. The transaction result is notified back to the backend application.
- The backend application notifies the web application about the new sensor data transaction being committed to the blockchain.
- The web application can query the latest data through a ledger query request to the backend application.
- The backend application queries the Fabric network using the SDK to retrieve the latest ledger data corresponding to the medicine storage environment.

- This query result containing the latest sensor readings is returned by the backend application to the web application for display and monitoring.

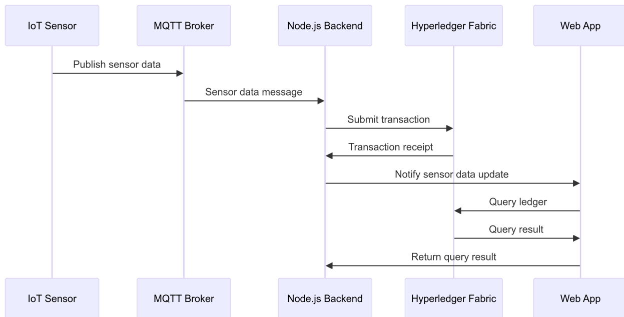

Fig. 4: Communication Sequence Diagram

IV. Blockchain and IoT Network Design

This section describes the overall system design, including the blockchain network, and IoT network components.

A. Blockchain Network Design

The Hyperledger fabric blockchain network is deployed using Docker containers for portability and isolation as shown in Fig:5. Key components include peer nodes, CouchDB databases, certificate authorities, ordering service, and CLI.

The network comprises two organizations - a hospital representing medicine storage facilities, and a regulator for oversight. Each organization operates a peer node and certificate authority, enabling decentralization. Peer nodes maintain ledgers and execute transactions, while regulators can audit by querying the nodes. This multi-organization model ensures privacy and access control between members of the consortium.

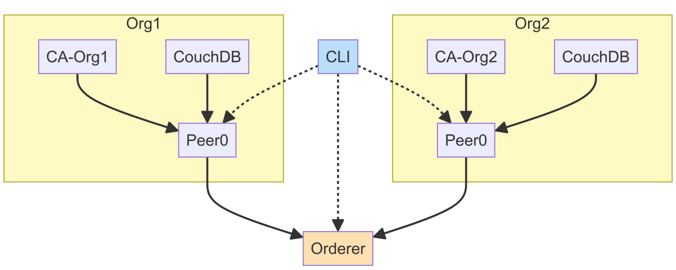

Fig. 5: Hyperledger fabric network docker containers

B. IoT Network Design

Raspberry Pi boards with sensors and communication technologies, such as Zigbee and LoRa, comprise the IoT network. The Raspberry Pi boards include temperature and humidity monitoring capabilities. It collects readings periodically, formats them into JSON, and transmits to the MQTT broker. For reliability, queued offline storage and synchronization mechanisms handle intermittent connectivity. This overall design facilitates seamless data transfer from IoT devices to the blockchain backend. Fig:6 Illustrates the design of the IoT network integrated with a blockchain network for proof-of-concept purposes.

In summary, the proposed system design realizes a decentralized architecture using permissioned blockchain for transparency and IoT sensors for granular supply chain monitoring.

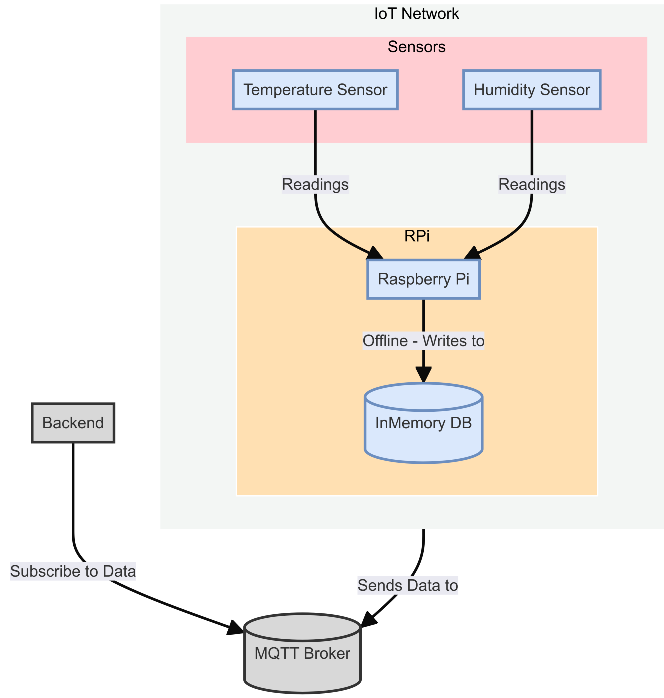

Fig. 6: IoT Network Design

C. System Deployment

The system implementation and deployment followed an incremental build process to realize the proposed architecture. Zigbee and LoRaWAN communication technologies were used for internal and external communication, respectively. The Hyperledger Fabric blockchain network was deployed first to establish the foundation for immutable data sharing. Docker containers enabled portability in setting up network entities like peers, CAs, and orderers. Cryptographic material defined member identities and access policies. Chaincode developed in Go provided core functions to store and retrieve sensor data on the distributed ledger.

With the blockchain network in place, the next phase focused on IoT integration. Raspberry Pi boards with sensors were configured to capture real-time readings. The Python application formatted the data and securely transmitted it to the MQTT message broker using encryption. Offline support ensured continuous data collection during network interruptions.

Finally, the Node.js backend application bridged the IoT devices and blockchain ledger. The Fabric SDK enabled transaction invocations to record sensor data on-chain. Express exposed an API endpoint to query the data. Integration with the MQTT broker allowed reliable transmission of real-time messages to the backend system components.

V. Performance Analysis

This section analyses the decentralized application's performance regarding transaction throughput and latency. Testing involved gradually increasing the number of IoT devices and securely transmitting their data through the blockchain network.

A. Transaction Throughput

In order to ensure the integrity of the test data, the total number of processed transactions was assessed against the expected quantity, calculated based on the duration of the test and the rate of transmission from the sensors in each phase:

- Phase 1: 30 sensors, each sending one message per second for 595 seconds, the expected result would be 17,850 transactions.
- Phase 2: 60 sensors, each sending one message per second for 596 seconds, the expected outcome would be 35,760 transactions.
- Phase 3: 120 sensors, each sending one message per second for 582 seconds, the expected number of transactions would be 69,840.

Fig:7 compares the total transactions processed versus the expected transactions based on the test duration and sensor transmitting. Throughput scaled from 30 transactions per second (TPS) in Phase 1 to 100 TPS in Phase 3 before degrading. At peak throughput, average CPU load reached 90% with some failed transactions, indicating capacity limitations (as shown in Fig:8). Total processed transactions matched expected values in Phases 1 and 2. However, Phase 3 saw a 16% failure rate, confirming system overload.

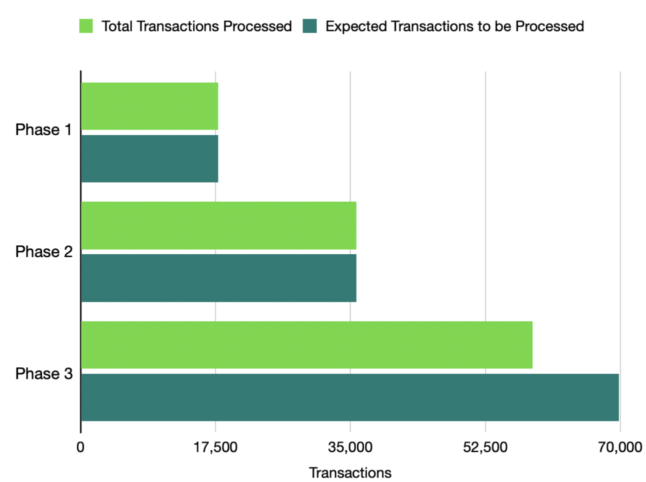

Fig. 7: Transactions Processed vs Expected

Higher throughput correlated directly with increased CPU usage. The analysis indicates approximately 100 TPS is the maximum sustainable throughput before performance degrades with the current deployment.

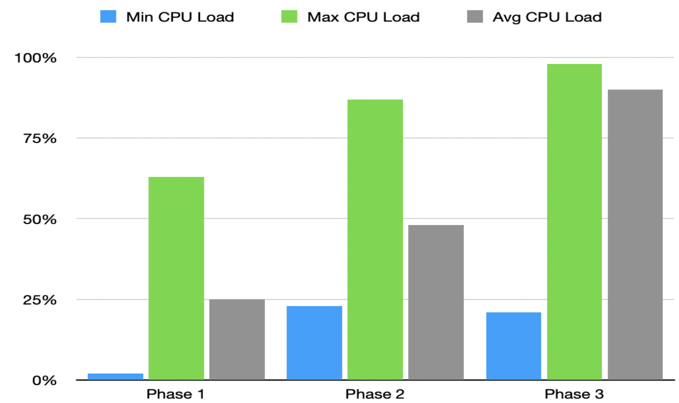

Fig. 8: CPU Load by Phase

B. Transaction Latency

Fig:9 shows the relationship between throughput and latency in our implementation. Latency remained under 500 ms for moderate transaction rates but spiked to over a minute when exceeding capacity at 270 TPS. High latency led to transaction timeouts.

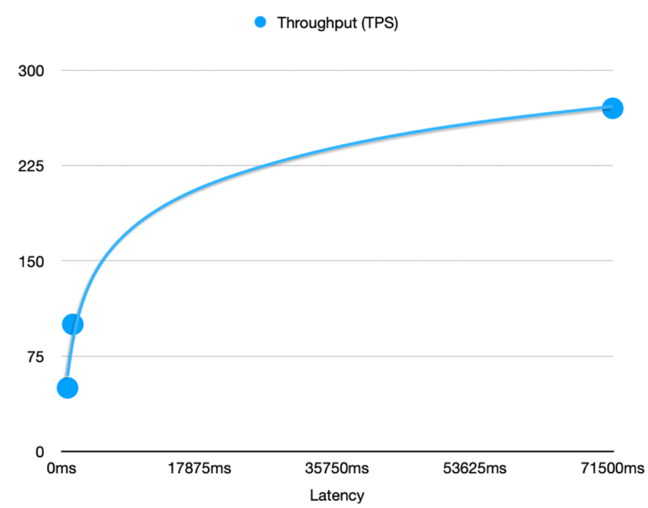

Fig. 9: Latency vs Throughput

Latency increases resulted from the system reaching processing capacity limits. Alterations to timeout thresholds could help but optimizing architecture is key to prevent high latency.

VI. Evaluation and Discussion

A. Summary of Key Findings

Through testing, the system's transaction throughput was found to scale effectively from 30 to 100 TPS, but with limitations. A peak CPU usage of 98% and the occurrence of transaction failures during the highest load indicated a capacity constraint. Additionally, latency remained low at moderate loads but significantly spiked when capacity was exceeded, corroborating the observed limitations on throughput.

B. Analysis of Technical Limitations

- **CPU Bottleneck:** High transaction loads led to CPU saturation, restricting scalability, and causing sharp latency increases.
- **Centralized MQTT Broker:** The design became a communication chokepoint under heavy loads, hindering the system from exploiting parallelism to its fullest extent.

C. Recommendations for Optimization

1) **Distribute Transaction Workload:** The bottleneck caused by the CPU saturation at high transaction loads suggests that the existing server configuration limits the system's ability to scale. This limitation could be mitigated by upgrading the server CPU or by distributing the workload across multiple servers (horizontal scaling), thus allowing more concurrent transactions.
2) **Decentralized Messaging:** Research by P. Jutadhamakorn et al. [8] demonstrated that distributing an MQTT broker across a cluster of Raspberry Pi devices with load balancing increased throughput and reduced latency compared to a single centralized broker under high message loads.
3) **Optimize Configurations:** The findings related to CPU utilization, latency, and throughput during various testing phases indicate that there may be room for improving resource efficiency within the existing architecture. Implementing a mechanism to batch transactions together can be an effective way to optimize resource usage. By limiting the data size and processing multiple transactions as a single batch, the system can reduce the number of individual requests to the CPU, thus improving efficiency.

The data indicates that system performance starts to degrade beyond 100 TPS. For more precise metrics on latency and throughput, implementing and evaluating the suggested optimizations is imperative.

VII. Conclusion

This paper presented the design and implementation of a blockchain and IoT-based middleware to address one of the challenges in pharmaceutical supply chain monitoring. The proposed solution aims to improve traceability, security and transparency of medicine storage conditions.

The decentralized architecture comprises Hyperledger Fabric permissioned blockchain, Raspberry Pi, sensors, MQTT messaging, and integration components. This enables tamper-proof and verifiable recording of temperature and humidity data from storage environments.

Performance analysis indicates the system can currently support workloads up to 100 transactions per second with reasonable latency. However, bottlenecks emerge at higher loads due to limited server resources and centralized message broker design.

The evaluation provides a quantitative baseline to guide future optimizations. Recommendations include distributing load across multiple servers, implementing decentralized messaging patterns, and transaction batching to improve efficiency.

While the current system offers promising capabilities, additional research and development focused on the suggested enhancements can help realize the full potential. Testing proposed changes using real-world supply chain data would provide further validation.

Acknowledgement

This work was supported by Sheffield Hallam University Department of Computing QR funding 2023-24.

References

[1] Mario Casillo, Liliana Cecere, Francesco Colace, Angelo Lorusso, and Domenico Santaniello. Integrating the internet of things (iot) in spa medicine: Innovations and challenges in digital wellness. *Computers*, 13(3), 2024.

[2] Michael Crosby, Pradhan Pattanayak, Sanjeev Verma, and Vignesh Kalyanaraman. Blockchain technology: Beyond bitcoin. *Applied Innovation*, 2(6-10):71, 2016.

[3] Polina Durneva, Kimberly Cousins, and Kun Chen. A systematic review of the applications of blockchain in health care. *Technology Innovation Management Review*, 10(9), 2020.

[4] Dereje G Feyisa, Adugna Jemal, Tsegaye Aferu, Fikru Ejeta, and Abebaw Endeshaw. Evaluation of cold chain management performance for temperature-sensitive pharmaceuticals at public health facilities supplied by the jimma pharmaceuticals supply agency hub, southwest ethiopia: Pharmaceuticals logistic management perspective using a multicentered, mixed-method approach. *Advances in Pharmacological and Pharmaceutical Sciences*, 2021, 2021.

[5] SMR Islam, Daehan Kwak, Humaun Kabir, Moshaddique Hossain, and Kyung-Sup Kwak. The internet of things for health care: a comprehensive survey. *IEEE access*, 3:678–708, 2015.

[6] Muhammad Aslam Jarwar, Sajjad Ali, and Ilyoung Chong. Exploring web objects enabled data-driven microservices for e-health service provision in iot environment. In *2018 International Conference on Information and Communication Technology Convergence (ICTC)*, pages 112–117, 2018.

[7] Muhammad Aslam Jarwar, Sajjad Ali, Inayatullah, and Sayed Chhattan Shah. Taking iot security to the next level: Hyperledger fabric private blockchain enabled iot middleware. In *2023 IEEE Globecom Workshops (GC Wkshps)*, pages 1325–1330, 2023.

[8] P. Jutadhamakorn, T. Pillavas, V. Visoottiviseth, R. Takano, J. Haga, and D. Kobayashi. A scalable and low-cost mqtt broker clustering system. In *2017 2nd International Conference on Information Technology (INCIT)*, pages 1–5, 2017.

[9] A Nokhodchi and Y Javadzadeh. The effect of storage conditions on the physical stability of tablets. *Pharmaceutical technology Europe*, 19(4):20–26, 2007.

[10] World Health Organization. Quality assurance of pharmaceuticals: a compendium of guidelines and related materials. vol. 2, good manufacturing practices and inspection. 2007.

[11] Achraf Rejeb, Jack Keogh, and Horst Treiblmaier. Leveraging the internet of things and blockchain technology in supply chain management. *Future Internet*, 11(7):161, 2019.

[12] MZ Uddin, W Khaksar, and Jim Torresen. Ambient sensors for elderly care and independent living: a survey. *Sensors*, 18(7):2027, 2018.

[13] Yuqian Xie, Jiajia Zhang, Huiru Wang, Ping Liu, Siyu Liu, Tongxue Huo, Yuxin Duan, et al. Applications of blockchain in the medical field: Narrative review. *Journal of Medical Internet Research*, 23(10), 2021.

[14] Mohammadreza Zamani and Paul Wembridge. Evaluating an automated temperature-monitoring system in medicine and vaccine storage facilities of a hospital network. *Asia Pacific Journal of Health Management*, 17(1):90–99, 2022.