A PROJECT REPORT

ON

"ANTI-COUNTERFEITING OF MEDICINE USING BLOCKCHAIN AND IOT "

Submitted to

BHARATI VIDYAPEETH
(DEEMED TO BE UNIVERSITY)
COLLEGE OF ENGINEERING, PUNE, INDIA

In Partial Fulfillment of the Requirement for the Award of

BACHELOR'S DEGREE IN
COMPUTER SCIENCE AND ENGINEERING
BY

Exam No: 2422390680 ADARSH KASHYAP PRN No: 2114110881

UNDER THE GUIDANCE OF
PROF. DR. BINDU GARG

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BHARATI VIDYAPEETH (DEEMED TO BE UNIVERSITY)
COLLEGE OF ENGINEERING, PUNE, INDIA - 411043

2023-2024

A PROJECT REPORT
ON

"ANTI-COUNTERFEITING OF MEDICINE USING BLOCKCHAIN AND IOT "

Submitted to

BHARATI VIDYAPEETH
(DEEMED TO BE UNIVERSITY)
COLLEGE OF ENGINEERING, PUNE, INDIA - 411043

In Partial Fulfillment of the Requirement for the Award of

BACHELOR'S DEGREE IN
COMPUTER SCIENCE AND ENGINEERING

BY

Exam No: 2422390680	ADARSH KASHYAP	PRN No: 2114110881

UNDER THE GUIDANCE OF
PROF. DR. BINDU GARG

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
BHARATI VIDYAPEETH (DEEMED TO BE UNIVERSITY)
COLLEGE OF ENGINEERING
PUNE, INDIA - 411043

2023-24

BHARATI VIDYAPEETH (DEEMED TO BE UNIVERSITY)
COLLEGE OF ENGINEERING
PUNE, INDIA-411043
2023-24

CERTIFICATE

This is certified that the project entitled

"ANTI-COUNTERFEITING OF MEDICINE USING BLOCKCHAIN AND IOT "

submitted by

Exam No: 2422390680	ADARSH KASHYAP	PRN No: 2114110881

is a record of bonafide work carried out by them, in the partial fulfillment of the requirement for the award of Degree of Bachelor of Technology in Computer Science And Engineering at Bharati Vidyapeeth (Deemed to Be University) College of Engineering, Pune, India. This work is done during academic year 2023-24

Date: 27 / 04 / 2024

Prof. Dr. Bindu Garg	Prof. Dr. Bindu Garg	
HOD, CSBS & CSE Engineering	Project Guide	External Examiner

Acknowledgements

We would like to express deepest appreciation towards Prof. Dr. Vidula Sohani, Principal, Bharati Vidyapeeth (Deemed to Be University) College of Engineering, Pune, India, and Prof. Dr. Bindu Garg, Head of Department of Computer Science and Engineering, who invaluable supported us in completing this project.

We are profoundly grateful to Prof. Dr. Bindu Garg, Project guide for his expert guidance and continuous encouragement throughout to see that this project rights, its target since its commencement to its completion.

At last, we must express our sincere heartfelt gratitude to all the staff members of the department of CSBS and CSE who helped me directly or indirectly during this course of work.

ADARSH KASHYAP

ABSTRACT

In an era marked by growing concerns over counterfeit pharmaceuticals and the need for enhanced medication security, our invention, titled "Anti-Counterfeiting Of Medicine Using Blockchain & IoT," stands as a groundbreaking solution. This innovation addresses the critical issues prevailing in the pharmaceutical industry, including the absence of blockchain technology, the lack of QR code integration, the need for fog architecture, data integrity concerns, and the inability to comprehensively track the pharmaceutical supply chain.

Counterfeit drugs pose a severe threat to public health, and ensuring the authenticity and safety of pharmaceutical products is of paramount importance. Our invention leverages the power of Blockchain and the Internet of Things (IoT) to create a robust, tamper-proof system that can significantly reduce the circulation of counterfeit medicines.

Our invention aims to provide an end-to-end solution that ensures medication security, real-time temperature monitoring, and comprehensive tracking of pharmaceutical products along the supply chain. The objectives include reducing counterfeit pharmaceuticals, improving temperature monitoring, enhancing transparency in the pharmaceutical supply chain, and ensuring data integrity.

Our invention offers several significant contributions to the pharmaceutical industry, including a substantial reduction in counterfeit drugs, enhanced temperature monitoring, increased supply chain transparency, and improved data integrity. The integration of blockchain and IoT technologies sets it apart from existing solutions.

Through the implementation of our system, we have achieved a comprehensive solution that addresses the vulnerabilities and challenges faced by the pharmaceutical industry, resulting in increased medication security and patient safety.

The potential applications of our invention extend across the pharmaceutical supply chain, including pharmaceutical manufacturers, distributors, pharmacies, and patients. It can also be utilized for temperature monitoring in clinical trials and the transportation of medical goods like blood products and vaccinations.

Keywords: Anti-Counterfeiting, Medicine, Blockchain, IoT, Medication Security, Temperature Monitoring, Pharmaceutical Supply Chain, Data Integrity, QR Code Integration, Fog Architecture, Counterfeit Drugs, Medication Authenticity

Contents

1 Introduction 1

1.1 Problem Definition 1

1.2 Motivation 2

1.3 Objective 2

2 Literature Survey 3

2.1 Literature Review 3

2.2 Comparative Analysis 5

3 Proposed Methodology 8

3.1 Technical Implementation and Infrastructure 8

3.2 Methodology, Verification, and Security 11

4 Software Requirements Specification 13

4.1 Functonal Requirements 13

4.2 Non-Functonal Requirements 14

5 Requirement Analysis 16

5.1 Functional Requirements 16

5.2 Non-Functional Requirements 16

6 System Design 18

6.1 System Design 18

7 System Testing 21

7.1 Test Cases and Test Results 23

8 Project Planning 24

8.1 Proposed Project Plan 24

8.2 Detailed Project Plan 25

9 Implementation 27

10 Screenshots of Results 37

10.1 Frontend 37

10.2 Backend 39

11 Conclusion and Future Scope 41

11.1 Conclusion 41

11.2 Future Scope 41

12 Research Publication 43

References 52

List of Figures

3.1 Blockchain Architecture 17

3.2 Interface Architecture 18

3.3 Fog Architecture 20

3.4 System Design 21

9.1 Deployed Contract 32

9.2 IoT Diagram 36

Chapter 1

Introduction

The convergence of Blockchain and Internet of Things (IoT) technologies has ushered in a new era in the battle against counterfeit medicines. This innovative approach ensures the integrity of pharmaceutical supply chains by leveraging the immutability of blockchain to securely record and track the journey of medications from production to consumption. By integrating IoT devices such as RFID tags and sensors, real-time data about the storage conditions and movement of medicines can be collected and authenticated. This synergy between Blockchain and IoT not only provides transparency and traceability but also enhances patient safety by mitigating the risks associated with counterfeit drugs. In this final year project report, we delve into the intricate mechanisms of this anti-counterfeiting solution, exploring its technical architecture, implementation challenges, and potential impact on healthcare systems worldwide.

Blockchain's decentralized ledger ensures the integrity and transparency of pharmaceutical supply chains by recording each transaction in an immutable and auditable manner. Meanwhile, IoT devices provide real-time monitoring of crucial parameters such as temperature, humidity, and location, thereby enabling immediate detection of any anomalies or unauthorized diversions. This multidimensional approach not only deters counterfeiters but also empowers consumers and regulatory authorities with verifiable information about the authenticity and provenance of medicines. Through this project, we explore the potential of this innovative solution to revolutionize the pharmaceutical industry and safeguard public health on a global scale.

1.1 Problem Definition

Counterfeit medicines pose a significant threat to public health worldwide, leading to harmful consequences such as ineffective treatment, worsening of health conditions, and even death. Traditional methods of tracking and verifying pharmaceuticals have proven insufficient in addressing this issue. Hence, there is a pressing need for innovative solutions to combat the proliferation of counterfeit drugs. This project aims to leverage the combined power of Blockchain technology and the Internet of Things (IoT) to develop a robust anti-counterfeiting system for medicines. The primary objective is to create a secure, transparent, and tamper-resistant supply chain network that enables stakeholders, including manufacturers, distributors, pharmacies, and consumers, to verify the authenticity of pharmaceutical products at every stage of the distribution process.

The proposed system will utilize IoT devices, such as RFID tags, sensors, and temperature monitors, to track the movement of medicines from production facilities to end-users in real-time. These devices will collect data on various parameters, including location, temperature, and handling conditions, and securely transmit it to the Blockchain network.

1.2 Motivation

Implementing blockchain and Internet of Things (IoT) technology for anti-counterfeiting of medicine presents a cutting-edge solution to a critical global issue. By harnessing the power of blockchain's immutable ledger and IoT's real-time data tracking capabilities, this project aims to safeguard the integrity of pharmaceutical supply chains, ensuring that patients receive authentic, safe, and effective medications. By combating the proliferation of counterfeit drugs, this innovative approach not only protects public health but also fosters trust and transparency within the healthcare ecosystem. Through this endeavor, we contribute to a safer and more reliable pharmaceutical industry, ultimately saving lives and improving overall well-being.

In recent years, the rise of counterfeit medicines has posed a significant threat to public health worldwide. These fraudulent pharmaceuticals not only undermine the efficacy of legitimate treatments but also endanger the lives of unsuspecting patients. Leveraging the combined power of blockchain technology and the Internet of Things (IoT) presents a transformative opportunity to address this pressing issue. By integrating blockchain's decentralized ledger system with IoT's sensor-based data collection and communication capabilities, we can create a robust and transparent supply chain ecosystem for pharmaceuticals. This approach enables real-time monitoring of the entire drug distribution process, from manufacturing to delivery, ensuring that each medication package is authentic and untampered with. By establishing an immutable record of transactions and product movements, blockchain technology enhances traceability and accountability, making it exceedingly difficult for counterfeiters to infiltrate the supply chain undetected.

1.3 Objective

The objective of this project is to develop a robust system leveraging blockchain technology and Internet of Things (IoT) devices to combat the pervasive issue of counterfeit medicines in the pharmaceutical supply chain. Counterfeit drugs pose significant risks to public health and safety, leading to detrimental consequences such as ineffective treatments, adverse reactions, and even fatalities. By integrating blockchain's immutable ledger and IoT's real-time monitoring capabilities, this project aims to establish a transparent and tamper-proof infrastructure for tracking pharmaceutical products from production to consumption. Through the implementation of smart contracts and sensor-enabled devices, the system will enable stakeholders to verify the authenticity and integrity of medicines at every stage of the supply chain, thereby ensuring patient safety and trust in the pharmaceutical industry.

Through the utilization of smart contracts, the system will automate processes and enforce compliance with regulatory standards, thereby reducing the likelihood of counterfeit products infiltrating the market. Furthermore, IoT devices equipped with sensors will facilitate the collection of real-time data on factors such as location, temperature, and humidity, allowing for enhanced traceability and quality control. Ultimately, this project seeks to instill confidence and trust in the pharmaceutical industry by ensuring the integrity and safety of medications through innovative technological solutions.

Chapter 2

Literature Survey

2.1 Literature Review

2.1.1 Review of existing models

Existing models for anti-counterfeiting of medicines utilizing blockchain and IoT offer innovative solutions to address the growing problem of counterfeit pharmaceutical products. These models typically leverage the inherent features of blockchain technology, such as immutability, transparency, and decentralization, along with the capabilities of IoT devices to create a robust and transparent supply chain ecosystem.

One prevalent model involves the integration of blockchain and IoT into track-and-trace systems, enabling stakeholders to monitor the movement of medicines from the point of manufacture to the end-user. Through the use of RFID tags, temperature sensors, and GPS trackers embedded in pharmaceutical packaging, real-time data about the location, temperature, and other relevant parameters of the products are collected and recorded on the blockchain. This ensures that each medicine's journey through the supply chain is transparent and traceable, allowing for quick identification of any anomalies or counterfeit products.

Furthermore, some models incorporate mechanisms for product authentication directly into the blockchain. By assigning unique digital identifiers to each medicine and storing them on the blockchain, consumers can verify the authenticity of the products using mobile apps or web portals. This not only empowers consumers to make informed decisions but also creates a deterrent for counterfeiters, as the authenticity of genuine products can be easily verified.

Another aspect of existing models is the focus on supply chain visibility. Blockchain and IoT enable supply chain stakeholders to gain real-time visibility into the movement and storage conditions of medicines, thereby enhancing transparency and accountability. By monitoring factors such as temperature, humidity, and handling conditions, stakeholders can ensure that medicines are stored and transported under optimal conditions to maintain their efficacy and safety.

Despite the promising potential of these models, several challenges persist. Scalability remains a significant concern, particularly when dealing with large-scale supply chains with high transaction volumes. Interoperability between different blockchain platforms and IoT devices also poses challenges for seamless data exchange and integration. Additionally, ensuring data privacy and security, as well as compliance with regulatory requirements, are crucial considerations in the implementation of these models.

2.1.2 Approaches

Approaches for combating the counterfeiting of medicines through the integration of blockchain and IoT technologies offer multifaceted solutions aimed at enhancing transparency, traceability, and authenticity throughout the pharmaceutical supply chain.

One approach involves the implementation of track-and-trace systems leveraging blockchain and IoT capabilities. In this approach, each pharmaceutical product is equipped with RFID tags, temperature sensors, and GPS trackers, allowing for real-time data collection on its journey from manufacturing facilities to end-users. These devices continuously monitor critical parameters such as location, temperature, and humidity, with data securely recorded on the blockchain. This ensures an immutable record of each medicine's movement, enabling stakeholders to trace its entire lifecycle and quickly detect any discrepancies or instances of counterfeit products infiltrating the supply chain.

Additionally, approaches may incorporate mechanisms for product authentication directly into the blockchain infrastructure. Through the assignment of unique digital identifiers to individual medicines, consumers and stakeholders can verify their authenticity using dedicated mobile applications or web-based platforms. By accessing the blockchain ledger, users can authenticate products in real-time, mitigating the risk of unwittingly purchasing counterfeit or substandard medications. This not only empowers consumers with information but also acts as a deterrent against counterfeiters, as the transparency and verifiability of genuine products become readily accessible.

Furthermore, approaches for anti-counterfeiting of medicines utilizing blockchain and IoT technologies emphasize the importance of supply chain visibility. By leveraging the data collected from IoT devices, stakeholders gain insights into the conditions under which medicines are stored, transported, and handled throughout the supply chain. Continuous monitoring of factors such as temperature, humidity, and storage conditions ensures compliance with quality standards and regulatory requirements, safeguarding the efficacy and safety of pharmaceutical products. This transparency fosters trust among stakeholders and facilitates rapid response to supply chain disruptions or quality issues, further bolstering the integrity of the pharmaceutical supply chain.

Despite the effectiveness of these approaches, challenges such as scalability, interoperability, data privacy, security, and regulatory compliance must be addressed to realize their full potential. Collaborative efforts between industry stakeholders, technology providers, and regulatory bodies are essential to overcoming these challenges and fostering the widespread adoption of blockchain and IoT-based solutions for anti-counterfeiting of medicines. By leveraging the combined strengths of blockchain and IoT technologies, these approaches hold promise in safeguarding public health and combatting the proliferation of counterfeit pharmaceutical products.

2.1.3 Problems

While the integration of blockchain and IoT technologies offers promising solutions for combating the counterfeiting of medicines, several significant challenges and problems need to be addressed to realize their full potential in ensuring the integrity of the pharmaceutical supply chain.

One major problem is scalability. Blockchain networks, particularly public ones like Bitcoin and Ethereum, face limitations in transaction processing speed and capacity. With the high volume of transactions involved in tracking pharmaceutical products throughout the supply chain, scalability issues may arise, leading to delays and congestion in transaction processing. Scalability solutions such as sharding, sidechains, or layer-2 protocols need to be explored and implemented to accommodate the scalability requirements of anti-counterfeiting initiatives effectively.

Interoperability between different blockchain platforms and IoT devices poses another challenge. The pharmaceutical supply chain involves multiple stakeholders, each potentially using different blockchain solutions or IoT technologies. Ensuring seamless data exchange and integration between these disparate systems is crucial for creating a unified and transparent supply chain ecosystem. Standardization efforts and interoperability protocols are needed to facilitate data interoperability and compatibility across various platforms and devices.

Data privacy and security are paramount concerns in anti-counterfeiting initiatives using blockchain and IoT. Pharmaceutical supply chain data, including information about product movements, storage conditions, and authentication records, are sensitive and confidential. Ensuring the privacy and security of this data against unauthorized access, manipulation, or breaches is essential to maintaining trust and integrity in the supply chain. Robust encryption, access control mechanisms, and data governance frameworks must be implemented to safeguard sensitive information throughout its lifecycle.

Regulatory compliance presents another challenge for anti-counterfeiting initiatives leveraging blockchain and IoT technologies. Pharmaceutical supply chains are subject to stringent regulations and standards imposed by regulatory authorities such as the FDA in the US and the EMA in the EU. Compliance with these regulations, including data integrity requirements, validation standards, and reporting obligations, adds complexity to the implementation of blockchain and IoT solutions. Ensuring that anti-counterfeiting initiatives align with regulatory requirements and standards is crucial to their acceptance and adoption by industry stakeholders and regulatory bodies.

Finally, cost considerations pose a significant barrier to the widespread adoption of blockchain and IoT-based anti-counterfeiting solutions in the pharmaceutical industry. Implementing and maintaining blockchain networks, deploying IoT devices, and integrating these technologies into existing supply chain infrastructures require substantial investments in terms of capital expenditure, operational costs, and technical expertise. Cost-effective deployment models, incentive mechanisms, and business models need to be developed to make anti-counterfeiting initiatives economically viable for pharmaceutical companies, especially smaller players with limited resources.

2.2 Comparative Analysis

2.2.1 Significance

The significance of utilizing blockchain and IoT technologies for the anti-counterfeiting of medicines cannot be overstated, as it addresses critical issues plaguing public health, safety, and trust in the pharmaceutical supply chain.

Firstly, counterfeit medicines pose a severe threat to public health worldwide. These fake or substandard products often lack the necessary active ingredients or contain harmful substances, jeopardizing patient safety and well-being. By leveraging blockchain and IoT technologies, anti-counterfeiting initiatives can ensure the authenticity and integrity of pharmaceutical products, thereby safeguarding patients from the risks associated with counterfeit medications.

Secondly, counterfeit medicines undermine trust in the healthcare system and pharmaceutical industry. Patients and healthcare providers rely on the authenticity and quality of medicines to treat various medical conditions effectively. The prevalence of counterfeit drugs erodes this trust and confidence, leading to skepticism and hesitation in

using pharmaceutical products. Implementing robust anti-counterfeiting measures using blockchain and IoT technologies helps restore trust and credibility in the pharmaceutical supply chain by providing transparency, traceability, and verifiability of medicines.

Furthermore, the economic impact of counterfeit medicines is substantial. Counterfeiting not only results in financial losses for pharmaceutical companies but also imposes indirect costs on healthcare systems and economies. The proliferation of counterfeit drugs leads to increased healthcare expenditures due to ineffective treatments, adverse health effects, and prolonged hospitalizations. By mitigating the circulation of counterfeit medicines through blockchain and IoT-based anti-counterfeiting initiatives, healthcare systems can reduce economic losses and allocate resources more efficiently towards improving patient care and public health.

Moreover, anti-counterfeiting efforts using blockchain and IoT technologies contribute to regulatory compliance and enforcement. Regulatory authorities such as the FDA, EMA, and WHO mandate stringent requirements for pharmaceutical product safety, quality, and traceability. Blockchain provides an immutable and auditable ledger for recording transactions and ensuring data integrity, while IoT devices enable real-time monitoring and surveillance of supply chain activities. By adhering to regulatory standards and enhancing visibility into the pharmaceutical supply chain, anti-counterfeiting initiatives facilitate compliance with regulatory requirements and support enforcement efforts against counterfeiters.

2.2.2 State of art review

A state-of-the-art review for the topic of anti-counterfeiting of medicines using blockchain and IoT reveals a dynamic landscape characterized by innovative solutions, ongoing research, and emerging trends aimed at enhancing the integrity and security of the pharmaceutical supply chain.

One prominent trend in recent years involves the integration of blockchain technology into anti-counterfeiting initiatives. Blockchain's decentralized and immutable ledger offers a robust platform for recording and verifying transactions related to pharmaceutical products, thereby creating a transparent and tamper-proof record of their movement throughout the supply chain. Various blockchain-based solutions have been developed, ranging from track-and-trace systems to product authentication mechanisms, to combat the proliferation of counterfeit medicines effectively.

In parallel, the adoption of IoT devices has gained traction in anti-counterfeiting efforts, enabling real-time monitoring and data collection in the pharmaceutical supply chain. IoT devices such as RFID tags, temperature sensors, and GPS trackers are deployed to track the location, temperature, and other critical parameters of medicines as they traverse the supply chain. This continuous monitoring enhances visibility, traceability, and accountability, facilitating the detection and prevention of counterfeit products.

Furthermore, state-of-the-art approaches for anti-counterfeiting of medicines leverage the synergies between blockchain and IoT technologies to create comprehensive and integrated solutions. These approaches combine the transparency and immutability of blockchain with the real-time data collection and monitoring capabilities of IoT devices to provide stakeholders with unprecedented insights into the movement and authenticity of pharmaceutical products. By seamlessly integrating blockchain and IoT functionalities, these solutions offer a holistic approach to combating counterfeit medicines and ensuring patient safety.

Recent research efforts have also focused on addressing key challenges and limitations associated with blockchain and IoT-based anti-counterfeiting initiatives. Scalability, interoperability, data privacy, security, regulatory compliance, and cost considerations remain areas of active investigation and innovation. Advanced techniques such as sharding, sidechains, zero-knowledge proofs, and homomorphic encryption are being explored to overcome scalability and privacy challenges, while interoperability standards and protocols are being developed to facilitate seamless data exchange between different blockchain platforms and IoT devices.

Chapter 3

Proposed Methodology

In this section, we propose a robust and comprehensive approach to address the challenges of counterfeit pharmaceuticals in the supply chain. This system combines blockchain and IoT technologies to enhance medication security, real-time temperature monitoring, and comprehensive tracking of pharmaceutical products. The key components of the solution include IoT sensors for temperature monitoring, blockchain for secure data storage, smart contracts for process automation, QR code integration, and the implementation of fog computing architecture for local data processing.

3.1 Technical Implementation and Infrastructure

3.1.1 Architecture

The system is built on a hybrid architecture combining blockchain and IoT components. Blockchain nodes are distributed across the pharmaceutical supply chain, including manufacturers, distributors, and pharmacies. IoT devices, equipped with temperature sensors and unique identifiers, are attached to individual medicine packages. These devices communicate with the blockchain network to record and verify transactions.

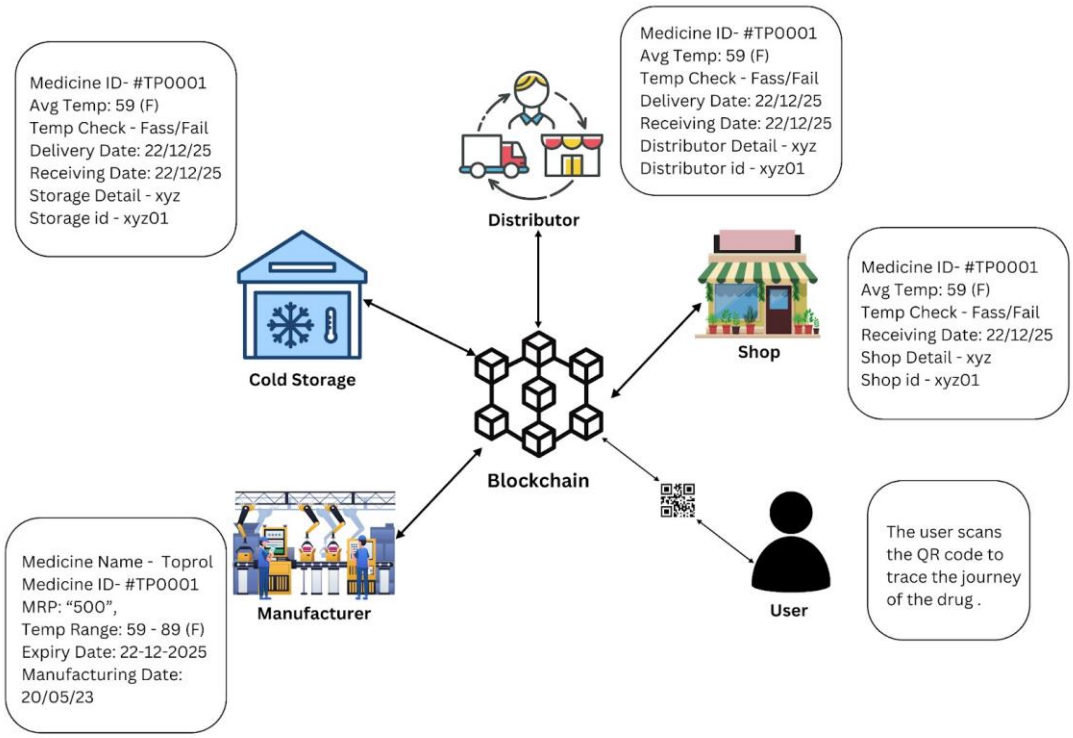

Fig. 3.1: Blockchain Architecture

3.1.2 Blockchain Implementation

A permissioned blockchain is employed to ensure data integrity and confidentiality among authorized participants. Smart contracts govern the rules for recording transactions and verifying the authenticity of medicines. Each transaction, representing a key event in the pharmaceutical supply chain, is cryptographically hashed and added to the blockchain, creating an immutable and transparent ledger. Using a permissioned blockchain for this anti-counterfeiting system offers many advantages over a traditional permissionless blockchain. By restricting access to only authorized users, blockchain permissions enhance data privacy and confidentiality, reducing the risk of sensitive information being released to unauthorized parties. This access-controlled system ensures that only accredited companies, such as pharmaceutical companies, distributors, and law enforcement agencies, can use the blockchain-enabled effective consensus mechanism because network participants are known entities, which allows for faster transaction processing and scalability.

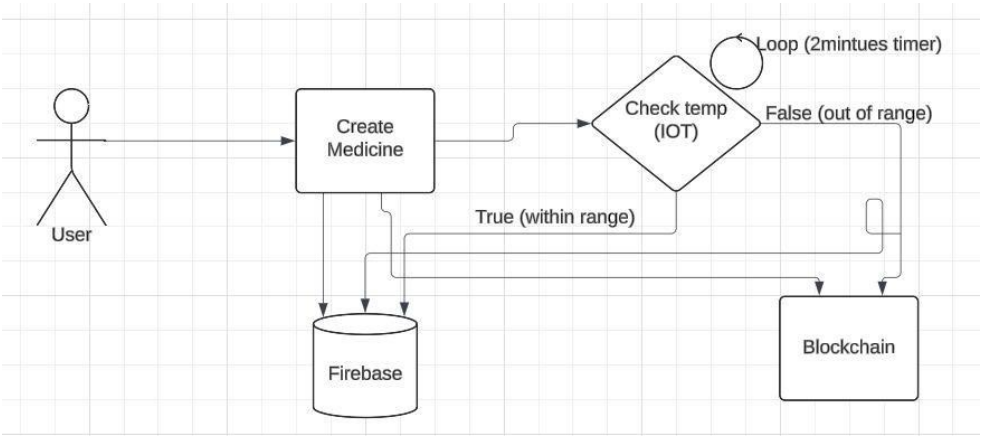

Fig. 3.2: Interface Architecture

3.1.3 IoT Devices

The IoT devices are embedded with temperature sensors to monitor the environmental conditions in which medicines are stored and transported. These devices are equipped with RFID or NFC technology for unique identification. Data collected by the IoT devices, including temperature readings and location information, is securely transmitted to the blockchain for real-time recording. The implementation of IoT devices with temperature sensors marks a significant leap forward in ensuring the integrity and safety of medicinal products throughout the supply chain. Imagine these devices as vigilant guardians, constantly monitoring the environment where medicines are housed and moved. With their temperature-sensing capabilities, they act as sensitive thermometers, meticulously tracking any fluctuations that could potentially compromise the effectiveness of medications. Whether stored in a warehouse or in transit, these IoT devices stand sentinel, providing invaluable insights into the conditions that directly impact the quality of pharmaceuticals.

3.1.4 Temperature Monitoring

The real-time temperature monitoring provided by the IoT devices ensures that pharmaceutical products are stored and transported within specified temperature ranges. Deviations from these ranges trigger alerts and are recorded on the blockchain, providing a transparent history of the temperature conditions throughout the product's journey. These

devices serve as the ever-watchful eyes, ensuring that medicines are cocooned within the optimal temperature ranges essential for maintaining their efficacy and safety. The transparency provided by real-time temperature monitoring extends far beyond mere surveillance. It paints a vivid picture of the journey undertaken by pharmaceutical products, capturing every twist and turn in their environmental conditions.

3.1.5 Fog Nodes for Local Data Processing

Fog nodes placed at strategic points within the supply chain can process the data collected by IoT devices. They can perform real-time analysis to detect anomalies, such as unexpected temperature fluctuations or deviations in the shipment's route. These nodes serve as local hubs for processing the wealth of data collected by IoT devices, acting as the first line of defense against potential threats to medication integrity. Nestled amidst the bustling activity of warehouses, distribution centers, and transit routes, these nodes are poised to sift through the deluge of information pouring in from the IoT sensors. Their role is akin to that of vigilant sentinels, tirelessly scanning for any signs of trouble lurking within the data streams.

With their formidable computing power and analytical prowess, fog nodes are not just passive bystanders; they're active participants in safeguarding the pharmaceutical supply chain. As the guardians of local data processing, they possess the capability to perform real-time analysis, swiftly identifying anomalies that could signal trouble. Whether it's a sudden spike in temperature or an unexpected deviation in the shipment's intended path, these nodes stand ready to sound the alarm, alerting stakeholders to potential risks before they escalate. By acting as the eyes and ears of the supply chain, fog nodes play a crucial role in maintaining the integrity and security of medicinal products, ensuring that they reach their destinations unscathed and ready to fulfill their life-saving purpose.

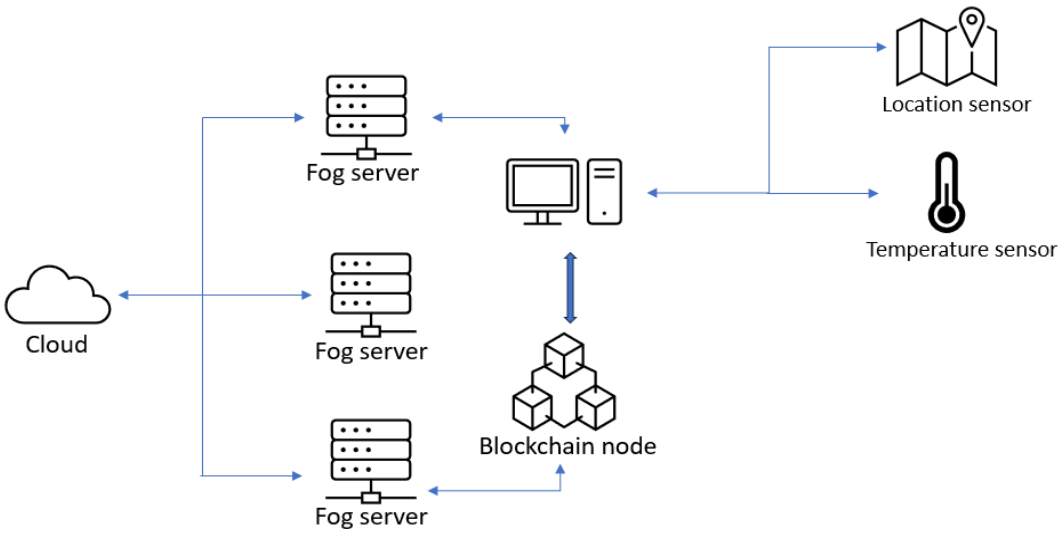

Fig. 3.3: Fog Architecture

3.2 Methodology, Verification, and Security

3.2.1 Verification at Each Node

As the medical products move through the supply chain, each node (e.g., distributors and pharmacies) can verify the authenticity of the products by checking their digital signatures against the blockchain records. Any discrepancy or counterfeit product can be immediately flagged for further investigation.

This verification process at each node within the supply chain not only ensures the authenticity of the medical products but also promotes accountability among stakeholders. Distributors and pharmacies can verify the legitimacy of the products they receive by cross-referencing digital signatures with blockchain records, thereby reducing the risk of inadvertently distributing counterfeit or substandard medication. Moreover, the transparency provided by blockchain technology fosters trust and collaboration among supply chain participants, as they can collectively monitor the movement of products and collaborate to address any issues or discrepancies encountered.

3.2.2 Data Security and Privacy

The use of encryption techniques and access controls ensures the security and privacy of sensitive data within the blockchain. Only authorized parties have access to specific information, maintaining confidentiality while allowing transparency within the supply chain. Within the blockchain-based anti-counterfeiting system, robust encryption techniques stand as the first line of defense against unauthorized access and malicious attacks. Picture encryption as an impenetrable fortress surrounding our data, rendering it unreadable to anyone without the proper decryption keys. This ensures that even if unauthorized parties were to gain access to the blockchain, they would be met with an insurmountable barrier, unable to decipher the encrypted information contained within.

3.2.3. Methodology for Proposed Work

The project employs a structural design approach to architect the system. The structural approach focuses on organizing the system's components and their interactions logically and efficiently. This approach allows us to ensure that the various elements of the system work together seamlessly to achieve the intended objectives. It involves designing the system's architecture, defining data structures, and specifying the functions and responsibilities of each component.

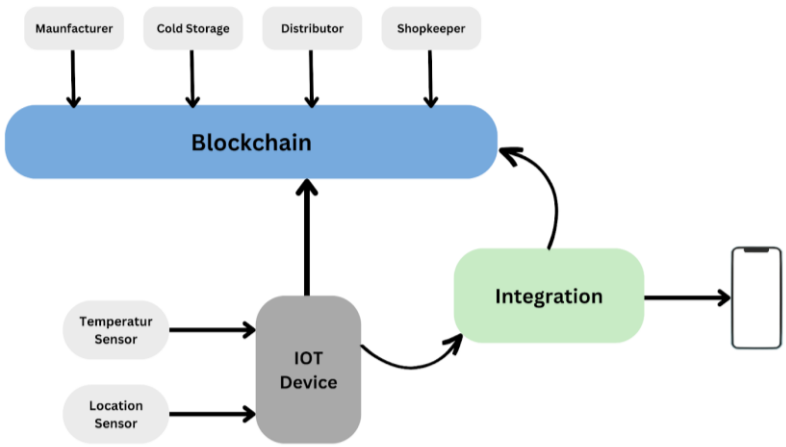

Fig. 3.4: System Design

3.2.4. Significance

The rampant proliferation of counterfeit medicine poses significant threats to global health, safety, and economic stability. In response, this research paper investigates the integration of blockchain technology and the Internet of Things (IoT) to combat counterfeit medicine effectively. This innovative approach not only addresses the immediate challenge of counterfeit drug proliferation but also establishes a foundation for a transparent and secure healthcare ecosystem. Through a comprehensive analysis of technological frameworks, implementation strategies, and potential challenges, this research paper provides valuable insights into the transformative impact of blockchain and IoT on anti-counterfeiting efforts in the pharmaceutical industry.

3.2.5. Novelty

The integration of blockchain and IoT technologies in the realm of anti-counterfeiting for medicine represents a novel and unique approach that holds immense promise. This research topic stands out for its innovative combination of two cutting-edge technologies to address a critical global issue. Blockchain's decentralized and immutable ledger provides a secure and transparent platform for tracking the entire lifecycle of pharmaceutical products, from manufacturing to consumption. IoT devices, on the other hand, enable real-time monitoring and data collection, enhancing the traceability and authenticity of medicines.

Chapter 4

Software Requirements Specification

4.1 Functional Requirements

4.1.1 Product Authentication

- The system should facilitate the assignment of unique digital identifiers to pharmaceutical products.
- It should allow stakeholders to authenticate products using these digital identifiers stored on the blockchain.

4.1.2 Track-and-Trace

- The system must enable real-time tracking of pharmaceutical products throughout the supply chain.
- It should record and maintain a transaction history of each product's movement on the blockchain.

4.1.3 QR Code Scanner

- The system must include a QR code scanning feature to enable stakeholders to authenticate pharmaceutical products easily. Users should be able to scan QR codes printed on product packaging using a smartphone or dedicated scanning device.
- The QR code scanner functionality is essential for quick and convenient authentication of pharmaceutical products. By scanning the QR code, stakeholders can access the product's digital identifier stored on the blockchain, allowing them to verify its authenticity and traceability within the supply chain. This feature enhances transparency, trust, and confidence in the legitimacy of medicines, helping to combat the threat of counterfeit products.

4.1.4 Create Medicine

- The system should provide functionality for authorized users, such as pharmaceutical manufacturers or authorized distributors, to create new medicine entries within the system. This feature involves inputting relevant information about the medicine, including its name, batch number, manufacturing date, expiry date, and other pertinent details.
- The ability to create new medicine entries is essential for maintaining an accurate and comprehensive record of pharmaceutical products within the anti-counterfeiting system. By creating a digital footprint for each medicine on the blockchain, stakeholders can establish a secure and immutable record of its provenance and authenticity. This feature enables stakeholders to track and trace medicines effectively throughout the supply chain, ensuring compliance with regulatory requirements and quality standards.

4.1.5 Send and Receive IoT Data from Server:

- The system should support the seamless transmission of IoT data between IoT devices (such as temperature sensors, RFID tags, and GPS trackers) and the server hosting the anti-counterfeiting system. IoT devices should be able to send real-time data to the server, including information about product conditions such as temperature, humidity, location, and other relevant parameters. The server should process and store this data securely, making it accessible to authorized stakeholders.
- The ability to send and receive IoT data from the server is critical for monitoring and ensuring the integrity of pharmaceutical products throughout the supply chain. By collecting real-time data from IoT devices embedded in product packaging, stakeholders can assess product conditions and detect any deviations from quality standards or potential tampering. This functionality enhances supply chain visibility, enabling stakeholders to take timely corrective actions to mitigate risks and safeguard patient health.

4.2 Non-Functional Requirements

4.2.1 Security:

- The system should implement robust security measures to protect sensitive data and prevent unauthorized access.
- Compliance with industry standards and regulations for data security, such as GDPR and HIPAA, is mandatory.

4.2.2 Scalability:

- The system must be scalable to handle the increasing volume of transactions and data generated by the supply chain.
- It should support high throughput and low latency to ensure smooth operation during peak demand.

4.2.3 Interoperability:

- The system should be interoperable with existing supply chain systems, allowing seamless integration and data exchange.
- Support for standard data formats and protocols is necessary to facilitate interoperability.

4.2.4 Usability:

- The system should have a user-friendly interface, making it easy for stakeholders to navigate and use effectively.
- Training and support should be provided to ensure stakeholders can utilize the system with ease.

4.2.5 Reliability:

- The system must be reliable, with minimal downtime and data loss, to ensure continuous operation.
- Backup and recovery mechanisms should be in place to safeguard against system failures and data corruption.

4.3 Use Cases

The anti-counterfeiting system utilizing blockchain and IoT technologies presents several use cases demonstrating its capabilities and functionalities:

4.3.1 Product Verification:

- A pharmaceutical distributor uses the system to verify the authenticity of incoming product shipments. By scanning the product's digital identifier with a mobile device, the distributor can access its transaction history on the blockchain, ensuring it originated from a legitimate source.

4.3.2 Temperature Monitoring:

- During transit, IoT sensors embedded in product packaging continuously monitor temperature conditions. If the temperature deviates from the specified range, an alert is generated and recorded on the blockchain, signaling potential quality issues or tampering.

4.3.3 Recall Management:

- In the event of a product recall, stakeholders can utilize the system to identify and trace affected products back to their source quickly. By querying the blockchain, manufacturers can identify which batches are affected and notify relevant parties, facilitating timely recall management.

4.3.4 Regulatory Compliance:

- Regulatory agencies can leverage the system to ensure compliance with pharmaceutical regulations and standards. By accessing the transparent and auditable transaction records on the blockchain, regulators can verify adherence to quality standards, serialization requirements, and distribution practices.

4.3.5 Supply Chain Optimization:

- Pharmaceutical companies can analyze data collected by the system to optimize supply chain processes and improve efficiency. Insights derived from blockchain and IoT data, such as transit times, storage conditions, and demand patterns, can inform decision-making and enhance overall supply chain performance.

Chapter 5

Requirement Analysis

5.1 Functional Requirements

5.1.1 Product Authentication:

Product authentication is crucial to combat the proliferation of counterfeit medicines, which pose significant risks to patient health and safety. By implementing a robust product authentication mechanism, the system ensures that only genuine pharmaceutical products enter the supply chain and reach end-users. This functionality is essential for protecting patients from counterfeit drugs, which may contain harmful ingredients or lack therapeutic efficacy, thereby safeguarding public health and maintaining trust in the pharmaceutical industry.

5.1.2 Track-and-Trace:

Track-and-trace functionality is essential for enhancing supply chain transparency, traceability, and accountability. By accurately recording the movement of pharmaceutical products from manufacturing facilities to end-users, the system enables stakeholders to trace the provenance and journey of each product. This capability is critical for detecting and mitigating risks such as counterfeit products, diversion, tampering, and theft. Additionally, track-and-trace functionality facilitates regulatory compliance, recall management, and optimization of supply chain operations, thereby improving efficiency and ensuring regulatory adherence.

5.2 Non-Functional Requirements

5.2.1 Security:

Security is paramount to protect sensitive supply chain data, prevent unauthorized access, and maintain the integrity and confidentiality of information. Given the high value and critical nature of pharmaceutical products, the system must implement robust security measures to safeguard against cyber threats, data breaches, and unauthorized modifications. Compliance with industry standards and regulations ensures that patient data privacy is upheld, and regulatory requirements are met. Security measures such as encryption, authentication, access control, and audit trails are essential for maintaining trust and confidence in the system's reliability and integrity.

5.2.2 Scalability:

Scalability is essential to accommodate the growing volume of transactions, data, and users within the pharmaceutical supply chain ecosystem. As the system expands to include additional stakeholders, products, and transactions, it must scale seamlessly to meet increasing demand without compromising performance or reliability. Scalability ensures that the system can handle peak loads, fluctuations in demand, and future

growth effectively. By supporting high throughput and low latency, the system can maintain optimal performance, responsiveness, and user satisfaction, thereby enhancing overall supply chain efficiency and effectiveness.

5.2.3 Interoperability:

Interoperability is critical to enable seamless integration and data exchange between the anti-counterfeiting system and other supply chain systems, stakeholders, and external partners. By adhering to interoperability standards and protocols, the system can communicate effectively with diverse systems, such as enterprise resource planning (ERP) systems, inventory management software, and regulatory databases. Interoperability ensures data consistency, accuracy, and reliability across the supply chain, facilitating collaboration, information sharing, and decision-making. By fostering interoperability, the system enhances supply chain visibility, transparency, and efficiency, ultimately improving patient safety and satisfaction.

5.2.4 Usability:

Usability is essential to ensure that stakeholders can interact with the anti-counterfeiting system intuitively, efficiently, and effectively. A user-friendly interface with clear navigation, intuitive design, and informative dashboards enhances user adoption, productivity, and satisfaction. Providing training, documentation, and support further empowers stakeholders to utilize the system optimally, reducing the learning curve and minimizing errors. Usability ensures that stakeholders can access, analyze, and act upon supply chain data seamlessly, thereby improving decision-making, collaboration, and overall system performance.

5.2.5 Reliability:

Reliability is fundamental to ensure continuous availability, performance, and integrity of the anti-counterfeiting system. Stakeholders rely on the system to provide accurate, timely, and consistent information about product authenticity, provenance, and condition. By implementing robust backup and recovery mechanisms, the system can mitigate the risk of data loss, system failures, and downtime, ensuring uninterrupted access to critical supply chain data. Reliability instills confidence in stakeholders and reinforces trust in the system's ability to safeguard patient health and safety effectively.

Chapter 6

System Design

6.1 System Design

6.1.1 Proposed Solution

Our proposed solution, "Anti-Counterfeiting Of Medicine Using Blockchain & IoT," introduces a robust and comprehensive approach to address the challenges of counterfeit pharmaceuticals in the supply chain. This system combines Blockchain and IoT technologies to enhance medication security, real-time temperature monitoring, and comprehensive tracking of pharmaceutical products. The key components of the solution include IoT sensors for temperature monitoring, Blockchain for secure data storage, smart contracts for process automation, QR code integration, and the implementation of fog computing architecture for local data processing.

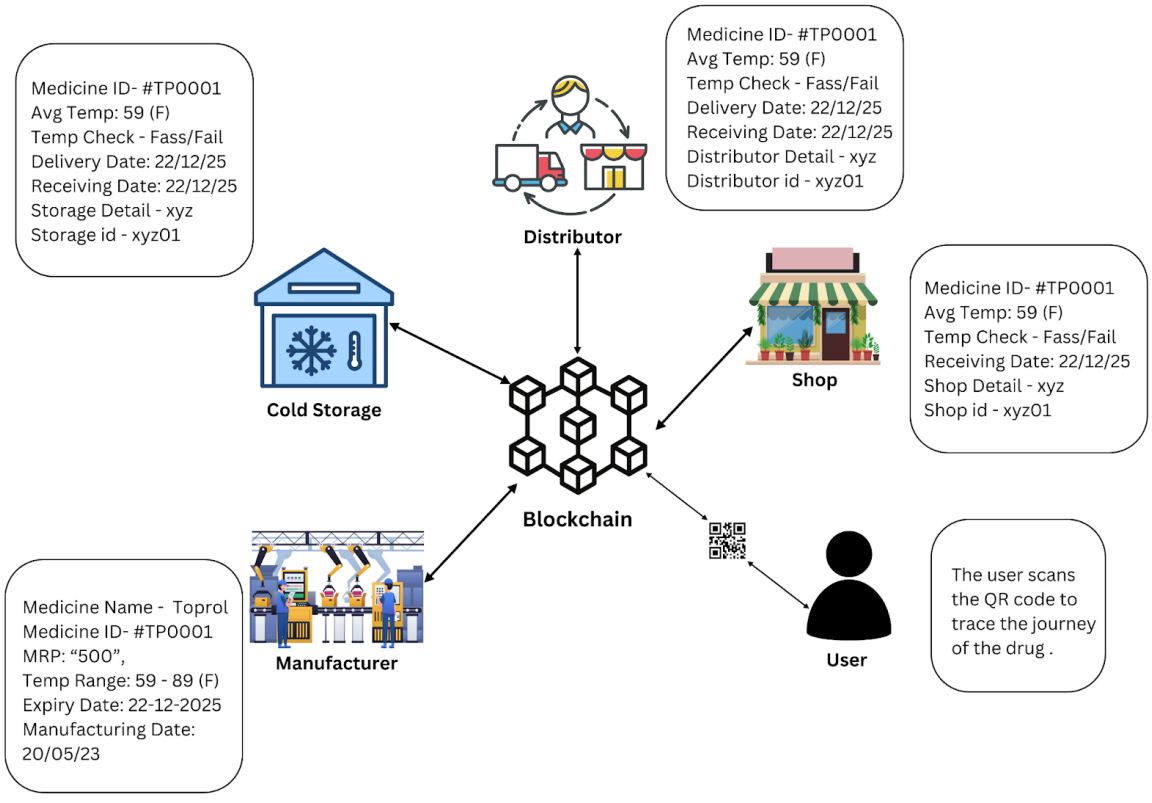

Figure 6.1: BLOCKCHAIN ARCHITECTURE

6.1.2 Design Approach

We employ a structural design approach to architect our system. The structural approach focuses on organizing the system's components and their interactions in a logical and efficient manner. This approach allows us to ensure that the various elements of our

system work together seamlessly to achieve the intended objectives. It involves designing the system's architecture, defining data structures, and specifying the functions and responsibilities of each component.

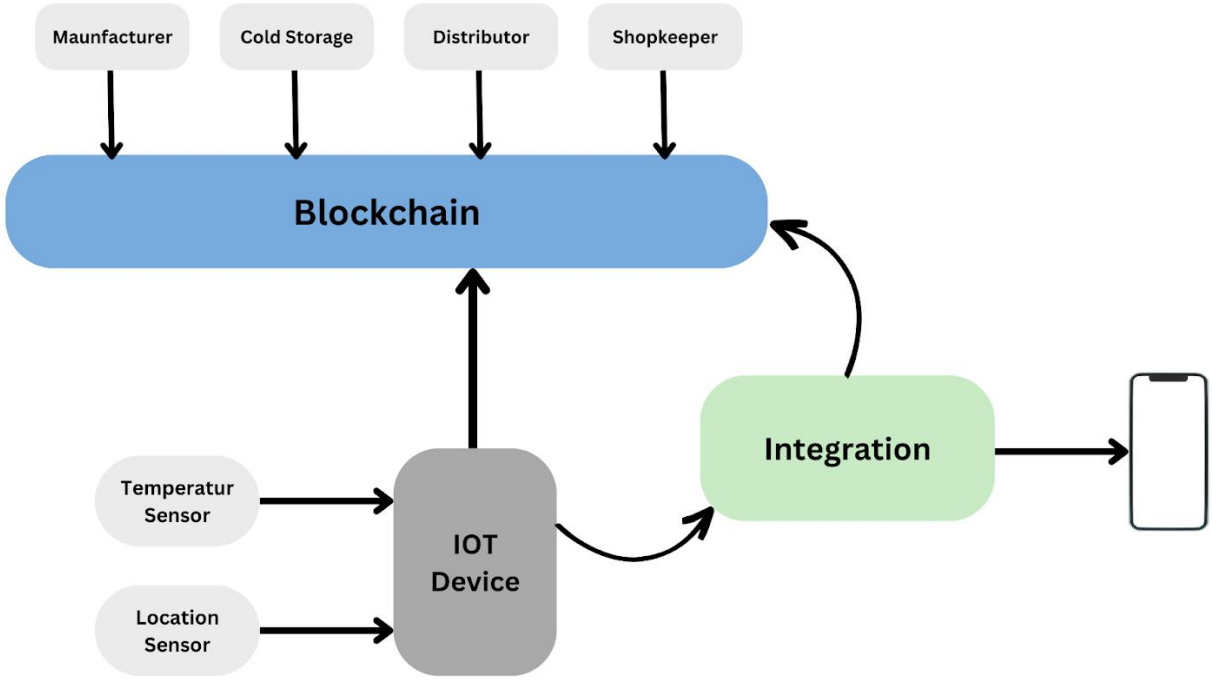

Figure 6.2: SYSTEM DESIGN

6.1.3 Design Tools Used: Introduction

In the design of our system, we utilize a range of software and tools to facilitate the development and implementation of the proposed solution. These tools include:

Blockchain Platforms: We leverage blockchain platforms such as Ethereum, Hyperledger Fabric, or Binance Smart Chain for implementing the secure and decentralized ledger for storing temperature data and ensuring data integrity.

IoT Development Tools: We employ IoT development tools and platforms like Arduino, Raspberry Pi, or specialized IoT development kits for creating and deploying IoT sensors for temperature monitoring.

Smart Contract Development: Smart contracts are a crucial part of our system, and we use tools like Solidity for Ethereum or Chaincode for Hyperledger Fabric to develop and deploy these self-executing contracts.

QR Code Generators: To create and manage QR codes on medication containers, we use QR code generation tools or libraries to encode essential product information.

Fog Computing Software: We utilize fog computing software for deploying fog nodes strategically across the supply chain to process temperature data in real-time. These can be designed using programming languages like Python.

6.1.4 Detailed System Design

The detailed system design involves the architectural and component-level design of our proposed solution. This includes defining the structure of the system, the interactions between components, and the data flow. The system design encompasses the following aspects:

Blockchain Structure: This defines the structure of the blockchain, including the creation of a unique digital signature or cryptographic hash for each pharmaceutical product to ensure authenticity.

IoT Sensor Placement: Specifies the strategic placement of IoT sensors within the supply chain for continuous temperature monitoring.

Smart Contract Logic: Outlines the logic and rules defined in the smart contracts to automate pharmaceutical supply chain processes.

QR Code Encoding: Describes the encoding of product information in QR codes, including manufacturer details, batch numbers, and expiration dates.

Fog Node Deployment: Specifies the deployment of fog nodes for local data processing to analyze temperature data and detect anomalies.

User Interface Design: Details the design of the user interface for scanning QR codes, allowing stakeholders and consumers to verify medication authenticity.

Chapter 7

System Testing

System testing for an anti-counterfeiting initiative focusing on medicines using blockchain and IoT involves a comprehensive process to ensure the reliability, functionality, security, and performance of the system. Here's a detailed outline of the system testing approach:

Functional Testing:

Verify that the system meets the specified functional requirements, including track-and-trace capabilities, product authentication mechanisms, and supply chain visibility features.

Test the functionality of blockchain components, such as smart contracts, transaction processing, and data storage, to ensure they operate as intended.

Validate the functionality of IoT devices and sensors for tracking, monitoring, and collecting data about pharmaceutical products throughout the supply chain.

Integration Testing:

Test the integration between blockchain and IoT components to ensure seamless communication and data exchange.

Verify that data collected from IoT devices is accurately recorded on the blockchain ledger and that smart contracts execute transactions correctly based on predefined conditions.

Validate the interoperability of the system with existing supply chain infrastructure, including enterprise resource planning (ERP) systems, inventory management software, and regulatory databases.

Security Testing:

Conduct security testing to identify and mitigate potential vulnerabilities, threats, and risks to the system.

Perform penetration testing to assess the resilience of the system against cyber-attacks, unauthorized access, and data breaches.

Verify that appropriate encryption, access control, and authentication mechanisms are implemented to protect sensitive data stored on the blockchain and transmitted by IoT devices.

Performance Testing:

Evaluate the performance of the system under normal and peak load conditions to ensure scalability, responsiveness, and reliability.

Test the throughput and latency of blockchain transactions, as well as the data collection and transmission rates of IoT devices, to assess system performance.

Identify any bottlenecks, latency issues, or resource constraints that may impact the system's ability to handle high volumes of transactions and data.

Usability Testing:

Assess the usability and user experience of the system, including user interfaces, dashboards, and mobile applications.

Gather feedback from stakeholders and end-users to identify usability issues, navigation challenges, and areas for improvement in user interaction and interface design.

Ensure that the system's features and functionalities are intuitive, accessible, and aligned with the needs and expectations of its intended users.

Regression Testing:

Conduct regression testing to ensure that new updates, enhancements, or bug fixes do not introduce unintended changes or regressions to existing functionality.

Re-run previously executed test cases and verify that the system behaves consistently and predictably across different versions and iterations.

Automate regression testing wherever possible to streamline the testing process and reduce the risk of human error.

Compliance Testing:

Validate that the system complies with relevant regulatory requirements, industry standards, and best practices for pharmaceutical supply chain management and anti-counterfeiting.

Ensure that data handling, storage, and transmission practices adhere to data privacy regulations such as GDPR, HIPAA, and CCPA.

Verify that the system meets specific regulatory mandates for pharmaceutical authentication, serialization, and traceability, such as those outlined by the FDA, EMA, and WHO.

Documentation and Reporting:

Document test cases, test results, and any issues or defects identified during testing.

Prepare comprehensive test reports summarizing the testing process, outcomes, and recommendations for further improvement or refinement.

Communicate testing results to stakeholders, project team members, and decision-makers, providing transparency and accountability throughout the testing phase.

7.1 Test Cases and Test Results

Test ID	Test Case Ttile	Test Condition	System Behavior	Expected Result	Actual Result
TC01	Dashboard Login	User attempts to log in	System allows login	User is logged in successfully	LoggedIn Successfully
TC02	Medicine Search	User searches for a medicine	System retrieves medicine information	Medicine information is displayed	Medicine Founded
TC03	View Medicine	User selects a medicine to view	System displays medicine details	Medicine details are displayed	Details displayed
TC04	Send data from IoT to blockchain	IoT device sends data to blockchain	Data is successfully transmitted	Data is transmitted to blockchain	Data sent
TC05	Receive data from blockchain	System receives data from blockchain	Data is successfully received	Data from blockchain is received	Data received
TC06	Scan QR Code	User scans a QR code	System retrieves medicine details	Medicine details are displayed after scanning	Scanned and displayed the details of medicine
TC07	Create Medicine	User creates a new medicine	System adds medicine to database	Medicine is successfully created	Medicine created
TC08	Scroll History	User scrolls through transaction history	All transactions are visible	User can view all transactions while scrolling	All transactions are visible when scrolling
TC09	Connect IoT with Wi-Fi	IoT device attempts to connect to Wi-Fi	Wi-Fi connection is established	IoT device successfully connects to Wi-Fi	Connection established
TC10	Send data from IoT to Firebase	IoT device sends data to Firebase	Data is successfully transmitted	Data is transmitted to Firebase	Data sent
TC11	Medicine Damaged if not in Temperature Range	Medicine is outside temperature range	System marks medicine as damaged	Medicine is marked as damaged	Marked as damaged

Chapter 8

Project Planning

8.1 Proposed Project Plan:

1. Initiation:
    - Define project objectives, scope, and stakeholders.
    - Formulate a project team with expertise in blockchain, IoT, pharmaceuticals, and project management.
    - Conduct a feasibility study to assess technical, financial, and regulatory aspects.
2. Requirement Gathering:
    - Identify anti-counterfeiting requirements, including track-and-trace, product authentication, and regulatory compliance.
    - Gather input from stakeholders through interviews, workshops, and surveys.
    - Analyze existing processes and systems within the pharmaceutical supply chain.
3. Technology Selection:
    - Evaluate blockchain platforms (e.g., Ethereum, Hyperledger) and IoT devices (e.g., RFID, temperature sensors).
    - Assess supporting technologies such as data analytics and machine learning.
    - Choose planning tools like Gantt charts, Kanban boards, and project management software.
4. System Design:
    - Develop a system architecture integrating blockchain and IoT components.
    - Design data models, smart contracts, and user interfaces.
    - Define protocols and standards for data exchange and interoperability.
5. Implementation:
    - Develop blockchain components, including smart contracts and transaction processing logic.
    - Deploy IoT devices for tracking and monitoring pharmaceutical products.
    - Integrate supporting technologies for data analysis and visualization.
6. Testing and Quality Assurance:
    - Conduct functional testing to verify system functionality.
    - Perform integration testing to ensure seamless communication between blockchain and IoT components.
    - Execute security testing to identify and mitigate vulnerabilities.
7. Deployment and Rollout:
    - Develop a deployment strategy, considering geographic regions and regulatory requirements.
    - Deploy the anti-counterfeiting solution in a phased approach, starting with pilot projects.
    - Provide training and support to stakeholders and end-users.
8. Monitoring and Optimization:
    - Implement monitoring tools and dashboards for tracking system performance.

- Collect feedback from stakeholders and end-users for continuous improvement.
- Iterate on the solution based on feedback and performance metrics.

8.2 Detailed Project Plan:

8.2.1 Phases

Phase 1: Initiation
- Objective: Define project scope, objectives, and stakeholders.
- Activities: Conduct feasibility study, form project team, define project plan.
- Deliverables: Project charter, stakeholder analysis, feasibility report.

Phase 2: Requirement Gathering
- Objective: Identify anti-counterfeiting requirements and gather stakeholder input.
- Activities: Conduct requirement workshops, analyze existing processes, document requirements.
- Deliverables: Requirements document, stakeholder feedback report.

Phase 3: Technology Selection
- Objective: Evaluate and select appropriate blockchain and IoT technologies.
- Activities: Research blockchain platforms and IoT devices, assess supporting technologies.
- Deliverables: Technology evaluation report, selection criteria matrix.

Phase 4: System Design
- Objective: Develop a comprehensive system architecture and design.
- Activities: Design system components, develop data models and user interfaces.
- Deliverables: System architecture diagram, data model documentation, UI wireframes.

Phase 5: Implementation
- Objective: Develop and deploy the anti-counterfeiting solution.
- Activities: Develop blockchain components, deploy IoT devices, integrate supporting technologies.
- Deliverables: Implemented solution, deployed blockchain network, integrated IoT devices.

Phase 6: Testing and Quality Assurance
- Objective: Verify system functionality, security, and performance.
- Activities: Conduct functional testing, integration testing, security testing.
- Deliverables: Test plans, test cases, test reports.

Phase 7: Deployment and Rollout
- Objective: Deploy the anti-counterfeiting solution and provide support to stakeholders.
- Activities: Develop deployment strategy, rollout pilot projects, provide training and support.
- Deliverables: Deployment plan, rollout schedule, training materials.

Phase 8: Monitoring and Optimization
- Objective: Monitor system performance and collect feedback for continuous improvement.
- Activities: Implement monitoring tools, collect stakeholder feedback, iterate on the solution.

- Deliverables: Monitoring dashboard, feedback analysis report, updated solution documentation.

8.2.2 Planning Tools Used:

- Gantt charts: for visualizing project timelines and dependencies.
- Kanban boards: for tracking tasks and workflow status.
- Project management software: for collaboration, task assignment, and progress tracking.
- Requirement management tools: for capturing, prioritizing, and managing project requirements.

Chapter 9

Implementation

The implementation of this project involved a meticulous setup of the development environment to facilitate seamless development. This included installing essential software and tools such as Node.js, React.js, Remix Studio, and Firebase. Once the necessary tools were in place, the development environment was configured to support frontend development using React.js and backend services using Firebase.

In the frontend development phase, React components were created to build the user interface, comprising pages dedicated to medicine registration, verification, and tracking. To ensure a visually appealing and user-friendly interface, CSS styling was implemented to enhance the frontend's visual appeal and usability, thus providing users with an intuitive experience.

The integration of blockchain technology was a pivotal aspect of the project. Smart contracts were developed using the Solidity language in Remix Studio. The main smart contract, named "MedicineContract.sol," was responsible for defining the structure and functions necessary for medicine registration, verification, and tracking on the blockchain. Key functions such as `registerMedicine`, `verifyMedicine`, and `trackMedicine` were implemented to interact with the blockchain. These smart contracts were compiled and deployed on the Ethereum blockchain network using Remix Studio's Ethereum virtual machine. Additionally, the React frontend was integrated with the deployed smart contracts using the Web3.js library, enabling seamless interaction with the blockchain.

In the backend development and database management phase, a Firebase project was configured to provide backend services, including Firestore for real-time database management. Backend services were implemented to handle user authentication and authorization using Firebase Authentication. A Firestore database schema was designed to securely store user data, medicine information, and transaction records.

The integration of IoT devices played a crucial role in the project. ESP32 microcontrollers were programmed using the Arduino IDE to collect sensor data from DHT11 (temperature and humidity) and GPS sensors. Communication protocols such as MQTT were established to securely send sensor data to fog nodes for local processing. Firmware was developed for ESP32 devices to transmit sensor data to fog nodes and trigger blockchain transactions based on predefined conditions, such as temperature thresholds.

Fog computing was utilized to enhance system responsiveness and reduce latency by processing data locally before interacting with the blockchain network. Fog nodes were configured to receive sensor data from IoT devices and perform local data processing. Logic was implemented on fog nodes to validate sensor data, execute smart contract functions for medicine registration and verification, and update blockchain state.

The deployment and hosting phase involved deploying the frontend React application to Firebase Hosting for public access. Backend services were hosted on Firebase Cloud Functions to handle server-side logic and integrate with the Firestore database. Smart

contracts were hosted on the Ethereum blockchain network for decentralized execution and immutable record-keeping.

Testing and quality assurance were integral parts of the implementation process. Unit tests were conducted for smart contracts to ensure proper functionality and behavior under different conditions. Frontend and backend components were tested for compatibility, usability, and security vulnerabilities. Integration tests were performed to verify the interaction between frontend, backend, blockchain, and IoT components, ensuring a robust and reliable system.

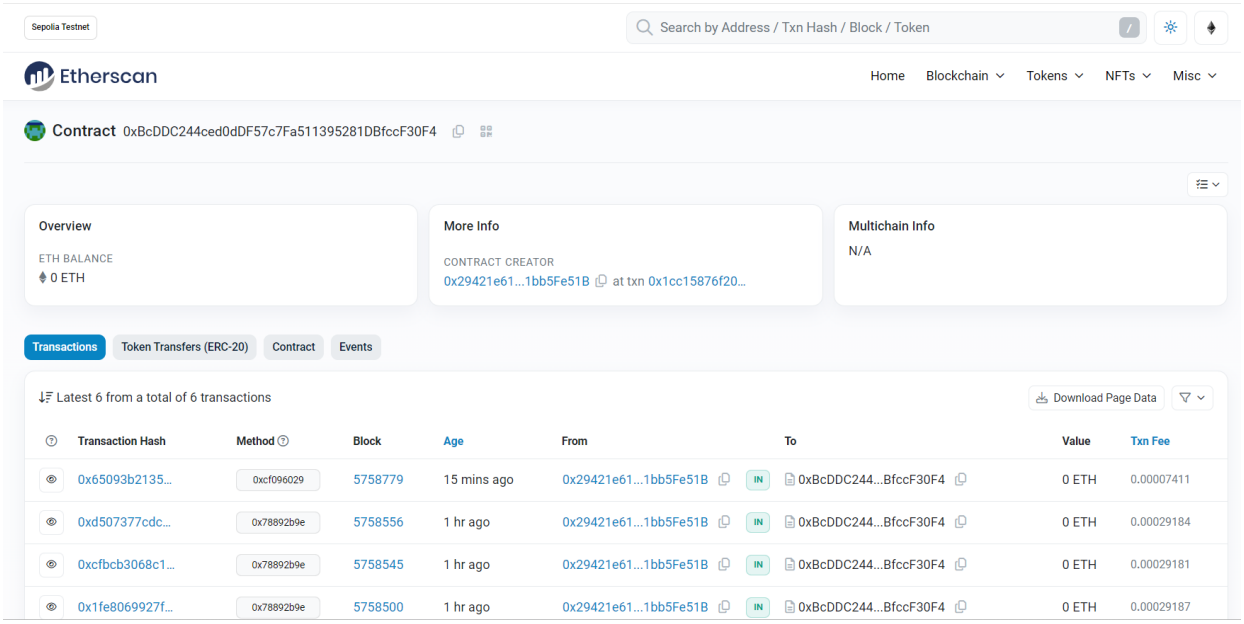

Figure 9.1: DEPLOYED CONTRACT

Code of Contract (In Solidity Language)-

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.24;

contract MedicineContract {
  // Structure to store medicine information
  struct Medicine {
    string name;
    uint256 minTemperature;
    uint256 maxTemperature;
    bool condition; // Initially true
    bool sold; // Initially false
    bytes32[] history; // Array to store history
    mapping(bytes32 => bool) historyExists; // Mapping to check existence of history
    mapping(bytes32 => HistoryDetail) historyDetails; // Mapping to store history details
  }

  // Structure to store detailed history information
  struct HistoryDetail {
```

```
        uint256 timestamp;
        uint256 currentTemperature;
        string location;
        int256 latitude;
        int256 longitude;
    }

    // Mapping to store medicine data by ID
    mapping(bytes32 => Medicine) public medicines;

    // Event emitted when a new medicine is added
    event MedicineAdded(bytes32 indexed id, string name, uint256 minTemperature, uint256 maxTemperature);

    // Event emitted when medicine history is updated
    event MedicineHistoryUpdated(bytes32 indexed id, uint256 timestamp, uint256 currentTemperature, string
location, int256 latitude, int256 longitude);

    // Function to initialize a new medicine
    function initializeMedicine(bytes32 id, string memory _name, uint256 _minTemperature, uint256
_maxTemperature) internal {
        Medicine storage newMedicine = medicines[id];
        newMedicine.name = _name;
        newMedicine.minTemperature = _minTemperature;
        newMedicine.maxTemperature = _maxTemperature;
        newMedicine.condition = true;
        newMedicine.sold = false;
    }

    // Function to add medicine
    function addMedicine(bytes32 _id, string memory _name, uint256 _minTemperature, uint256
_maxTemperature) external {
        require(medicines[_id].minTemperature == 0, "Medicine already exists");

        initializeMedicine(_id, _name, _minTemperature, _maxTemperature);
        emit MedicineAdded(_id, _name, _minTemperature, _maxTemperature);
    }

   // Function to add medicine history
    function addMedicineHistory(bytes32 _id, uint256 _currentTemperature, string memory _location, int256
_latitude, int256 _longitude) external {
        Medicine storage medicine = medicines[_id];
        require(medicine.minTemperature != 0, "Medicine does not exist");

        // Check if current temperature is within the range of min and max temperature
        // require(_currentTemperature >= medicine.minTemperature && _currentTemperature <=
medicine.maxTemperature, "Current temperature is out of range");

        bytes32 historyId = keccak256(abi.encodePacked(block.timestamp, _currentTemperature, _location,
_latitude, _longitude));
        require(!medicine.historyExists[historyId], "History already exists");

        medicine.history.push(historyId);
        medicine.historyExists[historyId] = true;

        // Store detailed history information
        medicine.historyDetails[historyId] = HistoryDetail(block.timestamp, _currentTemperature, _location,
_latitude, _longitude);
```

```
        emit MedicineHistoryUpdated(_id, block.timestamp, _currentTemperature, _location, _latitude, _longitude);

        // If current temperature is out of range, update medicine status to false
        if (_currentTemperature < medicine.minTemperature || _currentTemperature > medicine.maxTemperature)
{
            _updateMedicineStatus(_id, false);
        }
    }

    // Internal function to update medicine status
    function _updateMedicineStatus(bytes32 _id, bool _condition) internal {
        Medicine storage medicine = medicines[_id];
        require(medicine.minTemperature != 0, "Medicine does not exist");

        medicine.condition = _condition;
    }

    // Function to check if medicine exists by ID
    function medicineExists(bytes32 _id) external view returns (bool) {
        return medicines[_id].minTemperature != 0;
    }

    // Function to update medicine status
    function updateMedicineStatus(bytes32 _id, bool _condition) external {
        Medicine storage medicine = medicines[_id];
        require(medicine.minTemperature != 0, "Medicine does not exist");

        medicine.condition = _condition;
    }

    // Function to update medicine sold status
    function updateMedicineSoldStatus(bytes32 _id, bool _sold) external {
        Medicine storage medicine = medicines[_id];
        require(medicine.minTemperature != 0, "Medicine does not exist");

        medicine.sold = _sold;
    }

    // Function to get medicine details by ID
    function getMedicine(bytes32 _id) external view returns (
        string memory name,
        uint256 minTemperature,
        uint256 maxTemperature,
        bool condition,
        bool sold,
        bytes32[] memory history
    ) {
        Medicine storage medicine = medicines[_id];
        require(medicine.minTemperature != 0, "Medicine does not exist");

        return (
            medicine.name,
            medicine.minTemperature,
            medicine.maxTemperature,
            medicine.condition,
            medicine.sold,
```

```
            medicine.history
        );
    }

    // Function to get detailed history of a medicine by ID
    function getMedicineHistory(bytes32 _id) external view returns (HistoryDetail[] memory) {
        Medicine storage medicine = medicines[_id];
        require(medicine.minTemperature != 0, "Medicine does not exist");

        HistoryDetail[] memory details = new HistoryDetail[](medicine.history.length);
        for (uint256 i = 0; i < medicine.history.length; i++) {
            details[i] = medicine.historyDetails[medicine.history[i]];
        }
        return details;
    }
}
```

IOT Diagram-

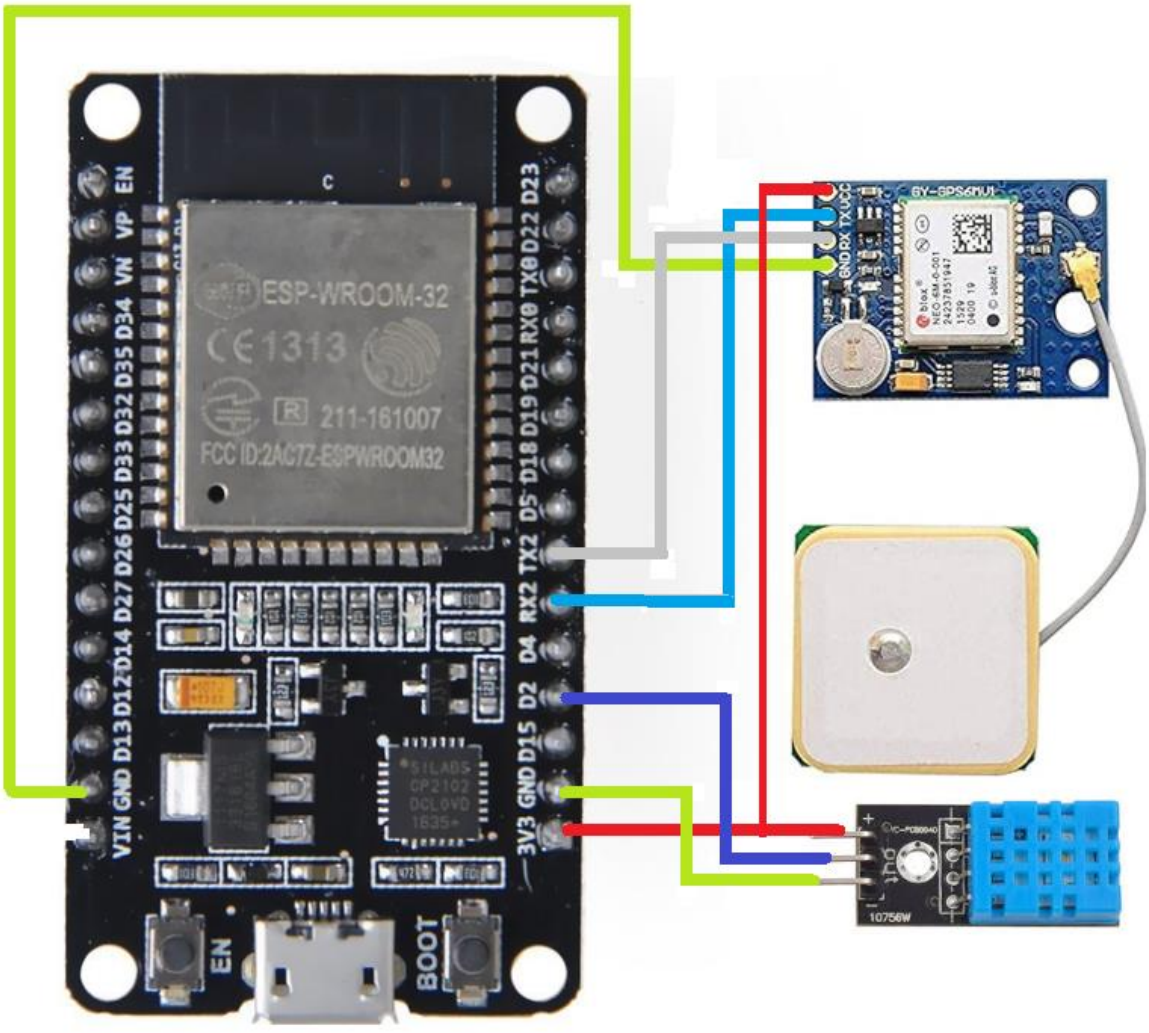

Figure 9.2: IoT Diagram

Code of IoT-

```
#include <DHT.h>
#include <WiFi.h>
#include <HTTPClient.h>
#include <ArduinoJson.h>
#include "time.h"
#include <HardwareSerial.h>
#include <TinyGPS++.h>

#define GPS_SERIAL Serial2  // Assuming GPS module is connected to Serial2 on ESP32

TinyGPSPlus gps;

#define DHTPIN 2     // Digital pin connected to the DHT11 sensor
#define DHTTYPE DHT11   // DHT 11

DHT dht(DHTPIN, DHTTYPE);

#define WIFI_SSID "WIFI_NAME"
#define WIFI_PASSWORD "WIFI_PASSWORD"

const char* projectId = “PROJECT_ID";
const char* privateKey = " PRIVATE KEY";

const char* medicineId = "0x1f1b48511f920c30de238b4050e32509d29b39a203252abfb3c05a0b4f5ee7f5";

const char* ntpServer = "pool.ntp.org";
const long  gmtOffset_sec = 0;
const int   daylightOffset_sec = 0;

WiFiClient client;
float maximumTemperature;
float minimumTemperature;
bool status=true;
void setup() {
  // Connect to Wi-Fi
  Serial.begin(9600);
  Serial.print("Connecting to ");
  Serial.println(WIFI_SSID);
  WiFi.begin(WIFI_SSID, WIFI_PASSWORD);
  while (WiFi.status() != WL_CONNECTED) {
    delay(500);
    Serial.print(".");
  }
  Serial.println("");
  Serial.println("WiFi connected.");

  // Initialize and get the time
  configTime(gmtOffset_sec, daylightOffset_sec, ntpServer);

  //To fetch details of medicine
  fetchMedicineData();
GPS_SERIAL.begin(9600);

}
void fetchMedicineData() {
    delay(2000);
```

```
  if (WiFi.status() == WL_CONNECTED) {
    HTTPClient http;

    // Construct Firestore URL
    String url = "https://firestore.googleapis.com/v1/projects/" + String(projectId) +
"/databases/(default)/documents/medicines/"+ String(medicineId) + "?key=" + String(privateKey);

    http.begin(url);

    // Send GET request to Firestore
    int httpResponseCode = http.GET();

    if (httpResponseCode > 0) {
      String response = http.getString();
      Serial.println(response);

      // Parse JSON response
      DynamicJsonDocument doc(1024);
      deserializeJson(doc, response);

      // Extract maximumTemperature and minimumTemperature from the response
      String maxTempStr = doc["fields"]["maximumTemperature"]["stringValue"];
      String minTempStr = doc["fields"]["minimumTemperature"]["stringValue"];
      status = doc["fields"]["status"]["booleanValue"];

      maximumTemperature = maxTempStr.toFloat();
      minimumTemperature = minTempStr.toFloat();

      Serial.print("Maximum Temperature: ");
      Serial.println(maximumTemperature);
      Serial.print("Minimum Temperature: ");
      Serial.println(minimumTemperature);
    } else {
      Serial.print("Error code: ");
      Serial.println(httpResponseCode);
    }

    http.end();
  } else {
    Serial.println("WiFi Disconnected");
  }
}


void loop() {
  delay(20000);

  float humidity = dht.readHumidity();
  float temperature = dht.readTemperature();
  fetchMedicineData();
getGPSData();
string latitude= gps.location.lat();
string longitude= gps.location.lng();
string location= gps.location();
if (!isnan(humidity) && !isnan(temperature)) {
      Serial.print("Date & Time: ");
      Serial.print(getFormattedTime());
      Serial.print(", Temperature: ");
      Serial.print(temperature);
```

```
    Serial.print(" °C, Humidity: ");
    Serial.print(humidity);
    Serial.println(" %");
    // Check if temperature is within range
    bool isTemperatureSafe = (temperature >= minimumTemperature && temperature <= maximumTemperature);
      // Update medicine status based on temperature range
       if(status){

         if(isTemperatureSafe){
            Serial.println("Medicine status is : safe ");
         }else{
            Serial.println("Medicine status is : Damaged ");
            updateMedicineStatus(isTemperatureSafe,temperature,humidity,latitude,longitude, location");
         }
       }
    sendTemperatureAndHumidity(temperature, humidity);
  } else {
    Serial.println("Failed to read from DHT sensor!");
  }
}

String getFormattedTime() {
 struct tm timeinfo;
 if(!getLocalTime(&timeinfo)){
  Serial.println("Failed to obtain time");
  return String("");
 }
 char buffer[30]; // Increased buffer size to accommodate timezone offset
 strftime(buffer, sizeof(buffer), "%Y-%m-%dT%H:%M:%SZ", &timeinfo);

 return String(buffer);
}

void sendTemperatureAndHumidity(float temperature, float humidity) {

 if (WiFi.status() == WL_CONNECTED) {
  HTTPClient http;

  // Construct Firestore document data
  DynamicJsonDocument doc(200);
  JsonObject data = doc.to<JsonObject>();
  data["fields"]["temperature"]["doubleValue"] = temperature;
  data["fields"]["humidity"]["doubleValue"] = humidity;
  data["fields"]["time"]["timestampValue"] = getFormattedTime();
  data["fields"]["latitude"]["stringValue"]="18.458328371701732";
  data["fields"]["longitude"]["stringValue"]="73.8551554319944";
  data["fields"]["location"]["stringValue"]="Pune";

  // Convert data to string
  String dataStr;
  serializeJson(doc, dataStr);

  // Construct Firestore URL
  String url = "https://firestore.googleapis.com/v1/projects/" + String(projectId) +
"/databases/(default)/documents/medicines/"+ String(medicineId) +"/transactions?key=" + String(privateKey);

  http.begin(url);
  http.addHeader("Content-Type", "application/json");

  // Send POST request to Firestore
```

```
    int httpResponseCode = http.POST(dataStr);

    if (httpResponseCode > 0) {
      Serial.print("HTTP Response code: ");
      Serial.println(httpResponseCode);
      String response = http.getString();
      Serial.println(response);
    } else {
      Serial.print("Error code: ");
      Serial.println(httpResponseCode);
    }

    http.end();
  } else {
    Serial.println("WiFi Disconnected");
  }
}

void updateMedicineStatus(bool isTemperatureSafe, float temperature, float humidity,String latitude, String
longitude,String location) {
  if (WiFi.status() == WL_CONNECTED) {
    HTTPClient http;

    // Construct Firestore document data
    DynamicJsonDocument doc(200);
    JsonObject data = doc.to<JsonObject>();
    data["fields"]["status"]["booleanValue"] = isTemperatureSafe;
    // Convert data to string
    String dataStr;
    serializeJson(doc, dataStr);

    // Construct Firestore URL
    String url = "https://firestore.googleapis.com/v1/projects/" + String(projectId) +
"/databases/(default)/documents/medicines/"+ String(medicineId) +
"?updateMask.fieldPaths=status&currentDocument.exists=true&key=" + String(privateKey);

    http.begin(url);
    http.addHeader("Content-Type", "application/json");

    // Send PATCH request to Firestore to update medicine status
    int httpResponseCode = http.PATCH(dataStr);

    if (httpResponseCode > 0) {
      Serial.print("Medicine status updated to: ");
      Serial.println("Damaged");
    } else {
      Serial.print("Error updating medicine status. Error code: ");
      Serial.println(httpResponseCode);
    }

    http.end();
  } else {
    Serial.println("WiFi Disconnected");
  }
}

void getGPSData() {
  if (GPS_SERIAL.available() > 0) {
    while (GPS_SERIAL.available() > 0) {
      gps.encode(GPS_SERIAL.read());
```

```
    }

    // Check if GPS data is valid
    if (gps.location.isValid()) {
      Serial.print("Latitude: ");
      Serial.println(gps.location.lat(), 6);
      Serial.print("Longitude: ");
      Serial.println(gps.location.lng(), 6);
    } else {
      Serial.print("Latitude: ");
      Serial.println(gps.location.lat(), 6);
      Serial.print("Longitude: ");
      Serial.println(gps.location.lng(), 6);
      Serial.println("Location data not available");
    }
  } else {
    Serial.println("GPS data not available");
  }
}
```

Chapter 10

Screenshots of Project

10.1 FRONTEND

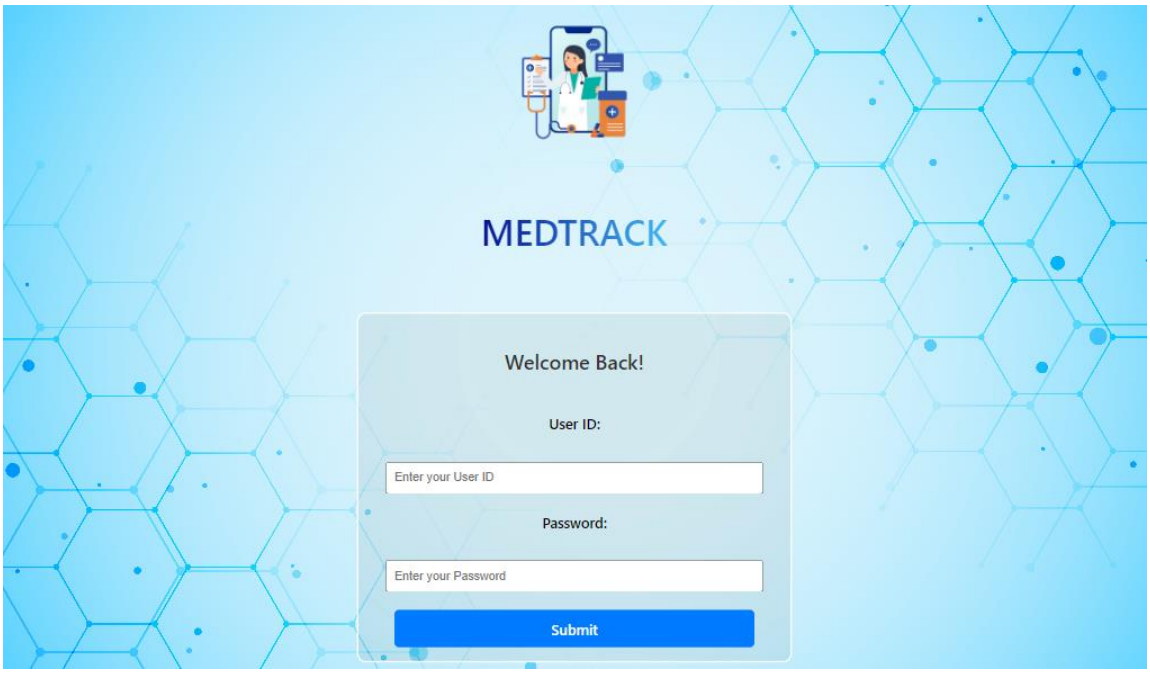

Figure 10.1.1: Login Screen

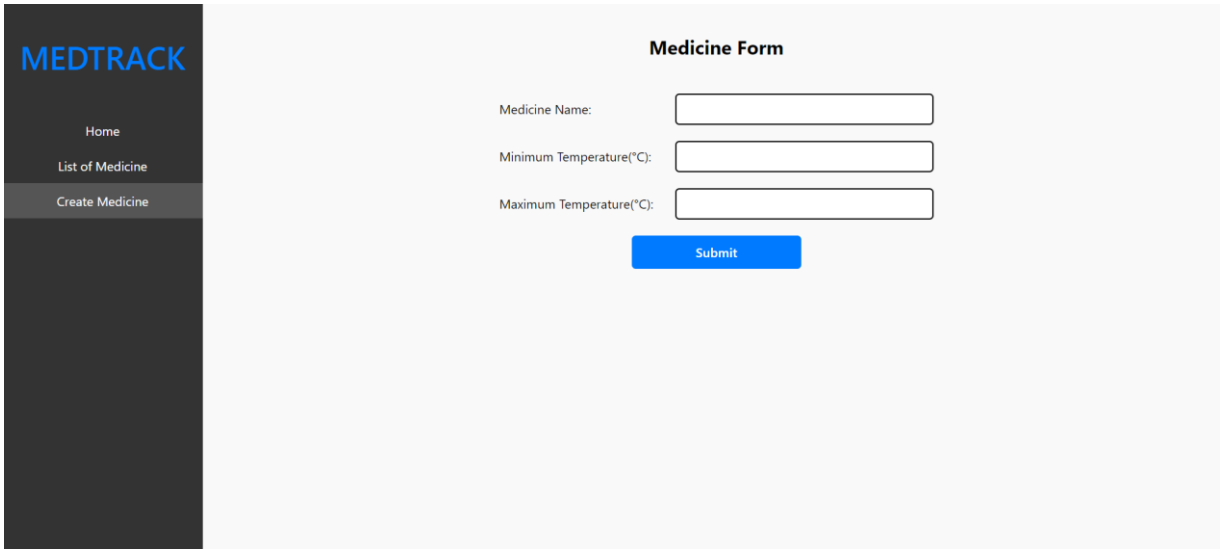

Figure 10.1.2: Medicine Form

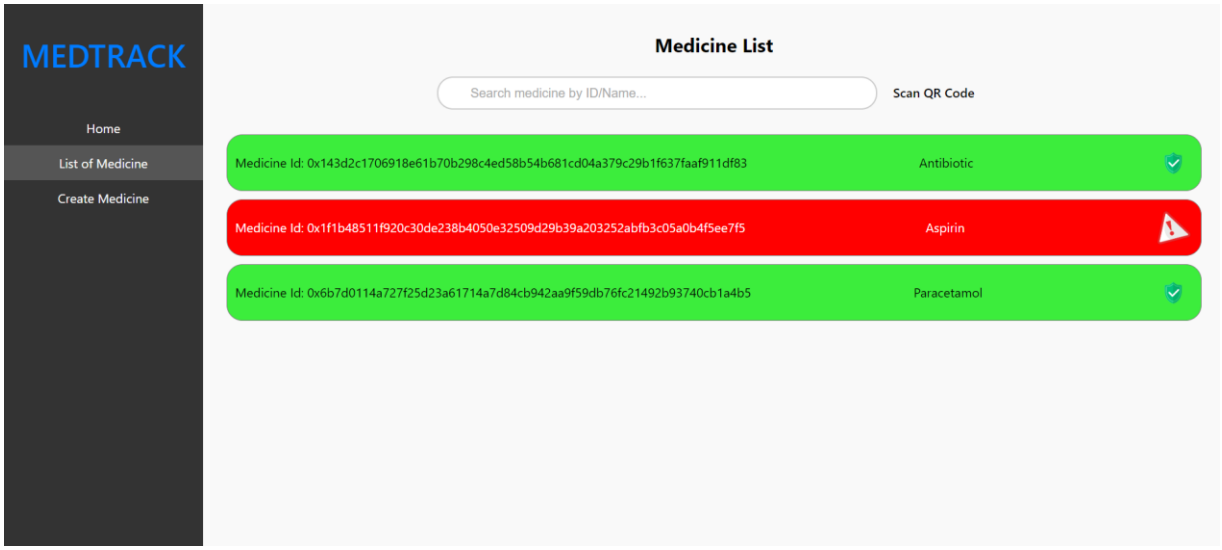

Figure 10.1.3: Medicine List

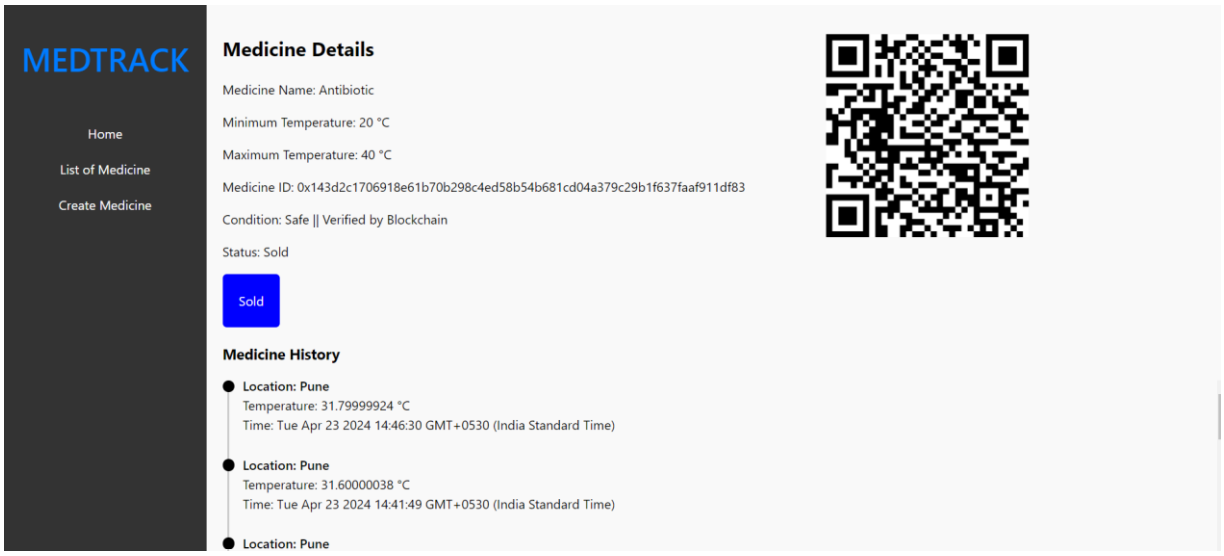

Figure 10.1.4: Medicine Details

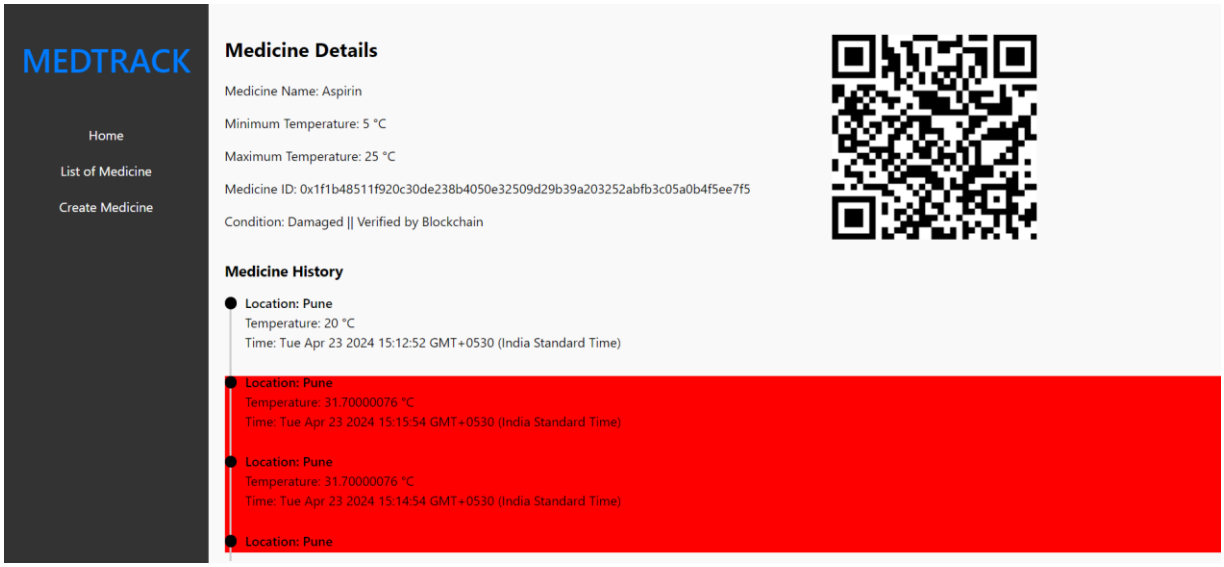

Figure 10.1.5: Damaged Medicine

10.2 BACKEND

Registration of medicine-

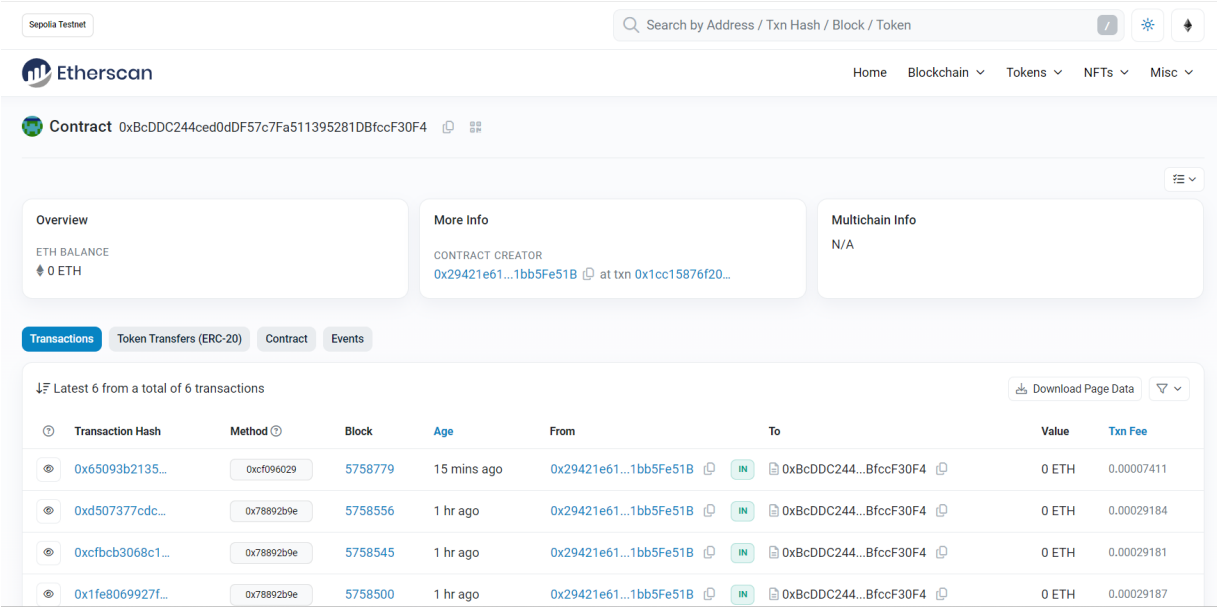

Figure: 10.2.1: Transaction Log on Blockchain

Data on Firebase-

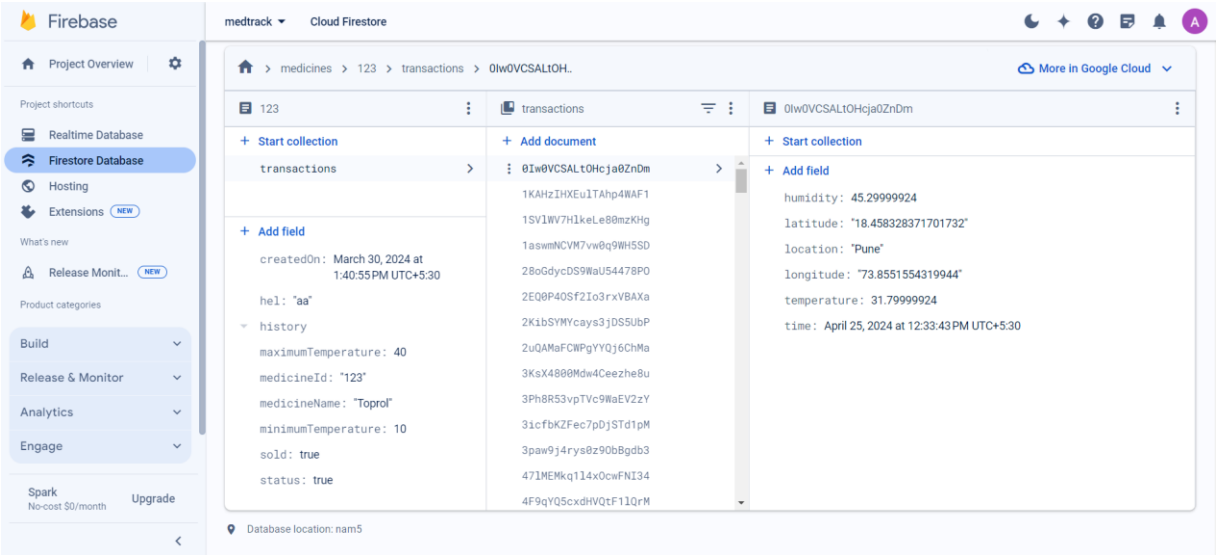

Figure: 10.2.2: Firebase dashboard

Arduino Console-

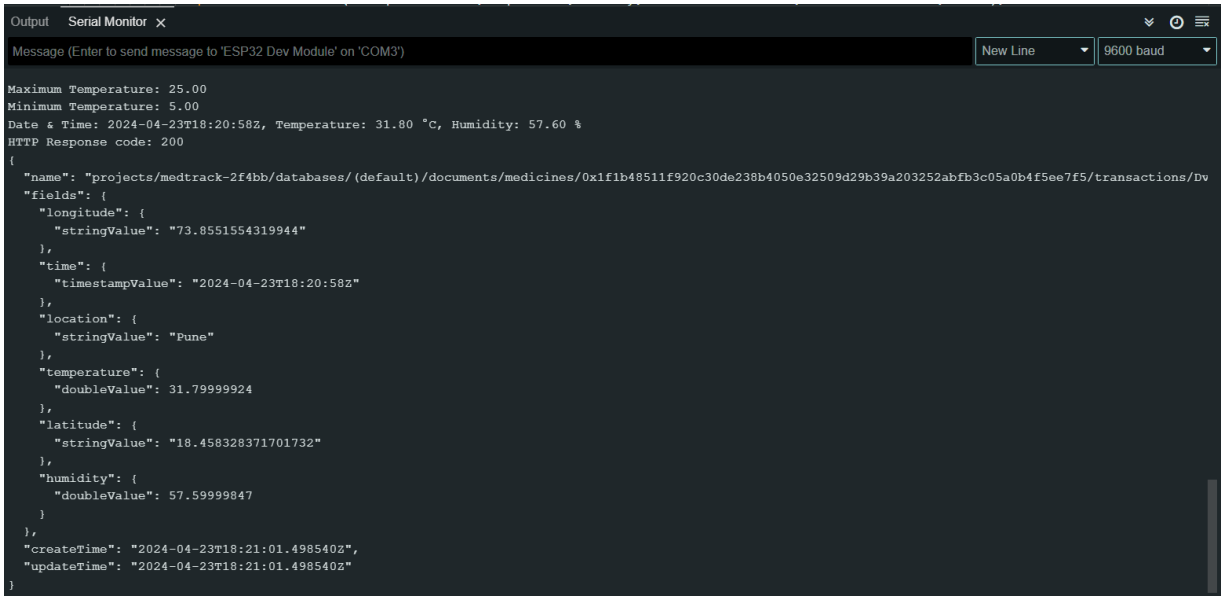

Figure: 10.2.3: Arduino Serial Monitor

Chapter 11

Conclusion and Future Scope

11.1 Conclusion

In conclusion, the integration of blockchain and IoT technologies presents a transformative solution to combat the proliferation of counterfeit medicines in the pharmaceutical supply chain. By leveraging the transparency, immutability, and traceability of blockchain, coupled with the real-time monitoring and data collection capabilities of IoT devices, anti-counterfeiting initiatives can significantly enhance supply chain integrity and patient safety.

Through blockchain, pharmaceutical stakeholders can establish a decentralized and tamper-proof ledger to record and verify the authenticity of medicines at every stage of the supply chain. This transparent record ensures that each pharmaceutical product's journey from production to consumption is securely documented, enabling stakeholders to detect and prevent counterfeit products effectively. Additionally, IoT devices provide real-time data on product conditions such as temperature, humidity, and location, enabling stakeholders to monitor and verify product authenticity throughout the supply chain.

The future of anti-counterfeiting initiatives using blockchain and IoT holds immense promise for further innovation and advancement. As scalability, interoperability, and security challenges are addressed, and complementary technologies such as AI, ML, and IoMT are integrated, anti-counterfeiting solutions will become even more robust and effective. By prioritizing security, privacy, and regulatory compliance, stakeholders can build trust and confidence in the authenticity and integrity of pharmaceutical products, ultimately safeguarding public health and ensuring the delivery of safe and effective medicines to patients worldwide.

11.2 Future Scope

The future scope for anti-counterfeiting of medicines using blockchain and IoT technologies is poised for significant advancements, promising to revolutionize the pharmaceutical industry's approach to supply chain integrity and patient safety.

One area of future development lies in the refinement and optimization of existing solutions. As blockchain and IoT technologies continue to evolve, improvements in scalability, interoperability, and efficiency will enhance the effectiveness of anti-counterfeiting initiatives. Scalability solutions such as layer-2 protocols and off-chain processing can address the throughput limitations of blockchain networks, enabling them to handle the high volume of transactions inherent in pharmaceutical supply chains. Similarly, advancements in interoperability standards and protocols will facilitate seamless integration between different blockchain platforms, IoT devices, and supply chain systems, enhancing data exchange and collaboration across stakeholders.

Another promising avenue for future development is the integration of complementary technologies to enhance anti-counterfeiting capabilities. Emerging technologies such as

artificial intelligence (AI), machine learning (ML), and the Internet of Medical Things (IoMT) can augment blockchain and IoT solutions by enabling advanced analytics, predictive modeling, and anomaly detection. AI and ML algorithms can analyze large datasets collected by IoT devices and blockchain to identify patterns indicative of counterfeit activity, enabling proactive detection and prevention of counterfeit medicines in the supply chain. Additionally, IoMT devices such as smart packaging and connected medical devices can provide real-time authentication and verification of pharmaceutical products, further bolstering supply chain security and transparency.

Furthermore, future anti-counterfeiting initiatives will prioritize security and privacy to safeguard sensitive data and protect against cyber threats. Advanced encryption techniques, zero-knowledge proofs, and decentralized identity management systems will be employed to ensure the confidentiality, integrity, and authenticity of pharmaceutical supply chain data. By implementing robust security measures, anti-counterfeiting solutions can mitigate the risk of unauthorized access, manipulation, or tampering, enhancing trust and confidence in the integrity of pharmaceutical products.

Overall, the future scope for anti-counterfeiting of medicines using blockchain and IoT technologies is characterized by ongoing innovation, collaboration, and technological advancements. By addressing scalability, interoperability, and security challenges while integrating complementary technologies, anti-counterfeiting initiatives will continue to evolve, ensuring the authenticity, safety, and efficacy of medicines in the global pharmaceutical supply chain.

Chapter 12

Research Publication

Anti-Counterfeiting of Medicine Using Blockchain & IoT

Adarsh Kashyap, Bindu Garg, Aryan Gavhankar, Swapnil J Singh, Shraddha Agarwal

Department of CSE,
Bharati Vidyapeeth Deemed University College of Engineering,
Pune, Maharashtra, India - 411043

adarshkashyap1muz@gmail.com
brgarg@bvucoep.edu.in
aryangavhankar12345@gmail.com
rajswapnil31@gmail.com
shraddhalive2629@gmail.com

Abstract*– This research presents an innovative methodology to address the challenges of counterfeit drugs and temperature monitoring in the pharmaceutical supply chain. The proposed approach integrates IoT devices for real-time temperature monitoring throughout the supply chain, with data securely stored on a tamper-proof and transparent blockchain. Smart contracts are employed to automate data management, ensuring compliance with temperature requirements and facilitating seamless drug tracking. Additionally, QR codes on drug packaging provide consumers with easy access to critical information, fostering transparency and empowering them to verify drug authenticity. The methodology stands out for its unique combination of blockchain and IoT technologies, utilization of smart contracts for automated tracking, and incorporation of QR codes for consumer engagement. The comprehensive solution offered by this methodology aims to prevent counterfeit drugs, ensure proper temperature conditions, enhance supply chain transparency, and empower consumers with valuable information.

Keywords: Anti-Counterfeiting, Medicine, Blockchain, IoT, Medication Security, Temperature Monitoring, Pharmaceutical Supply Chain, Data Integrity, QR Code Integration, Fog Architecture, Counterfeit Drugs, Medication Authenticity.

I. INTRODUCTION

The pharmaceutical industry plays a pivotal role in global healthcare, ensuring the production and distribution of essential medications. However, it faces a persistent threat in the form of counterfeit pharmaceuticals, which jeopardize public health and safety. Counterfeit drugs infiltrate the supply chain, posing significant challenges to medication security and authenticity. In response to this pressing issue, the research work introduces a novel approach, "Anti-Counterfeiting Of Medicine Using Blockchain & IoT," designed to enhance pharmaceutical security and integrity.

Counterfeit pharmaceuticals represent a serious concern in the pharmaceutical industry, with far-reaching consequences for both patients and stakeholders. The central problem revolves around the ease with which counterfeit medications can enter the supply chain, leading to potential harm and financial losses. Existing systems lack the robustness required to combat this menace effectively.

Counterfeit drugs pose a threat on many fronts, undermining the very foundation of trust upon which the healthcare system is built. Patients who inadvertently take counterfeit medicines face a myriad of risks ranging from ineffective treatment of diseases to serious side effects, the proliferation of counterfeit medicines undermines trust in the pharmaceutical industry, damages and tarnishes reputation, threatens the integrity of legitimate manufacturers and distributors.

Addressing the counterfeit drug problem requires a comprehensive and dynamic approach that goes beyond traditional resources. The research seeks to address this gap by leveraging the revolutionary potential of blockchain technology and the Internet of Things (IoT) to authenticate medication dispensing against counterfeiting. By leveraging blockchain's immutable ledger and IoT's real-time tracking capabilities, aim to transform drug safety, provide unprecedented stakeholder transparency and drive drug shipments and integrity on. Fog architecture facilitates real-time monitoring of medicine authenticity through distributed sensors at various points in the supply chain.Utilizing fog computing, blockchain, and IoT devices enhances traceability, ensuring each medicine's origin and journey is securely recorded. By leveraging fog architecture, stakeholders can access decentralized, tamper-resistant records, bolstering efforts to combat counterfeit drugs within the pharmaceutical industry. This new approach not only holds the promise of reducing the immediate risk of counterfeit medicines, but also lays the foundation for a robust and reliable pharmaceutical ecosystem, with patient safety and medicine of the most important integrity as well.

.

Motivation:- The primary motivation behind the research is the urgent need to address the rampant counterfeit drug issue. Public health is at stake, and ensuring the authenticity and safety of pharmaceutical products is of paramount importance. By leveraging the capabilities of Blockchain and the Internet of Things (IoT), the research aims to provide a robust, end-to-end solution that significantly reduces the circulation of counterfeit medicines. This research is driven by a strong commitment to improving medication security, real-time temperature monitoring, and comprehensive tracking of pharmaceutical products throughout the supply chain.

II. SIGNIFICANCE

The rampant proliferation of counterfeit medicine poses significant threats to global health, safety, and economic stability. In response, this research paper investigates the integration of blockchain technology and Internet of Things (IoT) to combat counterfeit medicine effectively. By leveraging blockchain's immutable ledger and IoT's real-time monitoring capabilities, the project aims to revolutionize the pharmaceutical supply chain, ensuring the authenticity and safety of medicinal products from production to consumption. This innovative approach not only addresses the immediate challenge of counterfeit drug proliferation but also establishes a foundation for a transparent and secure healthcare ecosystem. Through a comprehensive analysis of technological frameworks, implementation strategies, and potential challenges, this research paper provides valuable insights into the transformative impact of blockchain and IoT on anti-counterfeiting efforts in the pharmaceutical industry.

Furthermore, the integration of blockchain and IoT introduces unprecedented transparency and traceability into the pharmaceutical supply chain. Each transaction and movement of medicinal products are recorded on the blockchain, creating an immutable audit trail accessible to all authorized parties. IoT devices such as smart sensors and RFID tags enable real-time monitoring of various parameters such as temperature, humidity, and location, ensuring compliance with storage conditions and detecting any anomalies that may indicate tampering or counterfeit activities. This combination of technologies not only enhances the detection and prevention of counterfeit medicine but also facilitates rapid response mechanisms, allowing stakeholders to take immediate actions to mitigate risks and safeguard public health. Ultimately, the project aims to instill confidence among consumers, healthcare providers, and regulatory agencies by establishing a robust and trustworthy ecosystem for the pharmaceutical industry.

III. LITERATURE REVIEW

In this segment, we'll examine advancements in block chain technology and explore additional research on its utilization for traceability. Over the past few years, traceability has gained traction within supply chain management, extending across diverse production methods and product categories.

Several scholarly works and industry initiatives have addressed the potential of combining block chain and Internet of Things (IOT) technologies to revolutionize drug traceability and supply chain management within the pharmaceutical sector. Ahmad et al. (2019) delve into the advantages of harnessing block chain and IOT to monitor pharmaceuticals along the supply chain, emphasizing how these technologies can enhance traceability mechanisms and improve the detection of counterfeit products, thereby bolstering patient safety and regulatory compliance [1]

On a practical level, MediLedger (2019) represents a consortium of pharmaceutical companies actively employing block chain technology, as evidenced through the MediLedger initiative, which serves as a tangible example of the real-world implementation of block chain-based track and trace systems within the pharmaceutical industry [2]

Expanding on the logistical aspect, Dory et al. (2017) investigate the specific application of block chain and IOT in managing cold chain logistics for pharmaceuticals, highlighting their pivotal role in maintaining the integrity and efficacy of temperature-sensitive medications, which are susceptible to degradation under improper storage conditions [3]

Furthermore, Li et al. (2020) propose a comprehensive framework that integrates block chain and IOT to ensure the secure distribution of pharmaceuticals, underscoring the critical need for tamper-proof records and real-time monitoring to safeguard against counterfeit drugs and unauthorized tampering throughout the distribution process [4]

Lastly, Wang et al. (2019) contribute insights into the strategic considerations and essential success factors inherent in adopting block chain technology for supply chain traceability, with a particular emphasis on addressing the unique challenges and opportunities within the pharmaceutical domain. Together, these scholarly endeavors and industry endeavors underscore the transformative potential of block chain and IOT technologies in optimizing pharmaceutical supply chain operations and enhancing patient outcomes [5]

Multiple scholarly articles propose innovative solutions leveraging block chain and Internet of Things (IOT) technologies to tackle critical issues within the pharmaceutical sector. Khan et al. (2018) present a groundbreaking approach centered on block chain to combat the pervasive problem of counterfeit pharmaceuticals, ensuring the legitimacy and safety of medicinal products [6]

Lu et al. (2019) delve into the intricate realm of IOT sensors tailored for temperature monitoring within pharmaceutical supply chains, stressing their pivotal role in upholding optimal

storage conditions for medications, which is crucial for maintaining their efficacy and safety [7]

Meanwhile, Majid et al. (2019) conduct a comprehensive systematic review focusing on block chain's potential to revolutionize transparency and trust within clinical trials, which indirectly influences the integrity of pharmaceutical supply chains by bolstering confidence in the data generated from these trials [8]

Zeb et al. (2021) contribute a recent study that explores an integrated IOT and block chain system designed to safeguard the integrity and authenticity of pharmaceutical products, meticulously analyzing both the advantages and hurdles associated with implementing such a sophisticated solution [9]

Finally, Sinha et al. (2020) offer valuable insights into how block chain technology can serve as a robust tool for enhancing transparency across the entire pharmaceutical supply chain, thereby mitigating the grave risks posed by counterfeit medicines. Together, these scholarly endeavors underscore the increasing interest and ongoing efforts to harness the potential of block chain and IOT technologies in addressing multifaceted challenges within pharmaceutical supply chain management and product authentication [10]

IV. COMPARATIVE ANALYSIS

A comparative analysis involves a detailed examination and comparison of two or more entities, systems, theories, methods, or any other relevant subjects to identify similarities, differences, strengths, weaknesses, and patterns.

The paper titled "Securing the Pharmaceutical Supply Chain: A Block chain and IOT Integration Approach" explores the utilization of block chain and IOT technologies to address medicine counterfeiting in the pharmaceutical supply chain. It delves into the development and deployment of a secure system designed to monitor pharmaceutical movement from production to consumption. The advantages of this approach include improved traceability of pharmaceuticals, increased transparency within the supply chain, and a decreased risk of counterfeit medicines infiltrating the market. However, potential drawbacks include high implementation costs, the necessity for cooperation among various supply chain stakeholders, and scalability challenges, particularly in larger supply chains. Notably, the system lacks temperature and humidity monitoring capabilities [11]

The title of the paper is "Block chain -Based Anti-Counterfeit System for Pharmaceutical Products." The paper outlines a novel system leveraging block chain technology to combat counterfeit pharmaceuticals effectively. This system is designed to ensure the authenticity of pharmaceutical products by meticulously documenting their journey from production to distribution and ultimately to sale. A tamper-proof ledger, facilitated by block chain, serves as the foundation of this system, guaranteeing the integrity and immutability of recorded data. To facilitate the seamless operation of this system, Internet of Things (IOT) devices are employed to gather and transmit real-time data. Through the integration of block chain and IOT technologies, the system aims to establish a robust mechanism for verifying the legitimacy of pharmaceutical products, thereby enhancing consumer safety and bolstering trust within the pharmaceutical industry [12]

The paper titled "A Decentralized Approach to Medicine Authentication Using Block chain and IOT" introduces a pioneering system for authenticating medicines in a decentralized manner, leveraging block chain and IOT technologies. It delves into the concept of employing smart contracts to streamline the verification process, thereby diminishing the dependence on centralized entities. The proposed system aims to revolutionize medicine authentication by decentralizing control, thus mitigating the risks associated with relying solely on centralized authorities. Through the integration of block chain and IOT, the system seeks to establish a secure and transparent framework for validating the authenticity of medicines, ensuring consumer safety and fostering trust within the pharmaceutical ecosystem [13]

The research paper titled "Block chain-based drug supply chain provenance verification system" investigates the amalgamation of block chain technology and the Internet of Things (IOT) to address the pervasive issue of medicine counterfeiting. It delves into the utilization of IOT devices to meticulously monitor and trace the complete trajectory of medicines across the supply chain. By leveraging these IOT devices, the system can capture crucial data points at various stages, offering real-time insights into the movement and handling of pharmaceutical products.

Furthermore, the paper underscores the pivotal role of block chain technology in ensuring the integrity and transparency of the collected data. Through the implementation of block chain, the system establishes an immutable ledger that securely records and verifies each transaction and interaction within the supply chain. This tamper-proof ledger serves as a repository of truth, enabling stakeholders to authenticate the provenance of medicines with confidence.

By harnessing the combined power of block chain and IOT, the proposed system endeavours to enhance the resilience of drug supply chains against counterfeit activities, thereby safeguarding public health and bolstering trust among consumers and stakeholders within the pharmaceutical industry [14]

The research paper titled "Practical Anti-Counterfeit Medicine Management System Based on Block Chain Technology" is anticipated to introduce a pragmatic solution that harnesses block chain technology to tackle the pervasive problem of counterfeit medicines. It is likely to delve into the intricacies of designing, implementing, and applying a

practical system aimed at tracking and validating the authenticity of pharmaceutical products across the supply chain.

This system is expected to leverage the inherent features of block chain, such as its immutable ledger, to create a transparent and secure record of each medicine's journey from production to distribution and ultimately to the end consumer. Through the utilization of smart contracts, the paper may propose automated protocols that facilitate verification processes, reducing human intervention and enhancing efficiency.

Furthermore, the paper may discuss the potential integration of Internet of Things (IOT) devices to enable real-time monitoring and data collection throughout the supply chain. These IOT devices could provide crucial insights into various aspects of the pharmaceutical ecosystem, such as temperature control, transportation conditions, and product handling.

By providing insights into the design, implementation, and practical application of such a system, the research paper aims to offer a comprehensive approach to combating counterfeit medicines. Through the seamless integration of block chain technology and possibly IOT devices, the proposed solution strives to bolster transparency, trust, and accountability within the pharmaceutical industry, ultimately safeguarding public health and well-being[15]

V. IMPORTANT TECHNOLOGY

The Internet of Things (IoT) encompasses a network of interconnected devices embedded with sensors, software, and other technologies, enabling them to collect and exchange data over the internet. From smart home appliances to industrial machinery and urban infrastructure, IoT devices are proliferating rapidly, reshaping how we interact with the physical world. IoT technology facilitates real-time monitoring, automation, and optimization of processes, leading to increased efficiency, productivity, and convenience across diverse domains.

In parallel, Blockchain technology has emerged as a distributed ledger system that enables secure, transparent, and immutable record-keeping of transactions. Unlike traditional centralized databases, blockchain operates on a decentralized network of nodes, ensuring that data remains tamper-proof and resistant to censorship. The cryptographic principles underlying blockchain ensure the integrity and authenticity of transactions, fostering trust and transparency in digital interactions.

The integration of IoT and Blockchain offers a myriad of opportunities for innovation and disruption. One of the primary challenges in IoT ecosystems is ensuring the security and privacy of data generated by interconnected devices. By leveraging blockchain's decentralized architecture and cryptographic features, IoT data can be securely stored, validated, and shared among authorized parties. Blockchain enables the creation of immutable audit trails, enhancing transparency and accountability in data transactions.

Moreover, blockchain-based smart contracts can automate and enforce agreements between IoT devices, facilitating seamless and trustless interactions without the need for intermediaries. This capability streamlines processes such as supply chain management, logistics, and asset tracking, reducing costs and minimizing errors.

As the IoT landscape continues to evolve and expand, the integration of blockchain technology will play a pivotal role in addressing critical challenges related to data security, interoperability, and trust. Collaborative efforts between industry stakeholders, researchers, and policymakers are essential to unlock the full potential of IoT and blockchain and drive meaningful innovation in the digital era.

A. Ethereum Blockchain

Ethereum is a decentralized platform that enables the creation of smart contracts and decentralized applications (DApps). It provides a robust infrastructure for deploying and executing smart contracts, making it well-suited for implementing anti-counterfeiting solutions in the pharmaceutical industry.

In this research, Ethereum serves as the underlying blockchain technology. Smart contracts deployed on the Ethereum blockchain facilitate the tracking and authentication of pharmaceutical products throughout the supply chain. Each medicine package is assigned a unique identifier that is stored on the blockchain, along with relevant information such as manufacturing details, batch numbers, and expiration dates.

B. Solidity Programming Language

Solidity is a programming language used for writing smart contracts on the Ethereum blockchain. It is specifically designed to facilitate the creation of secure and reliable smart contracts, allowing developers to implement complex logic and business rules for pharmaceutical supply chain management.

C. Web3.js

Web3.js is a JavaScript library that allows interaction with Ethereum nodes and smart contracts from web applications. It enables developers to build user-friendly interfaces for interacting with blockchain-based systems, facilitating the integration of anti-counterfeiting solutions into existing pharmaceutical supply chain workflows.

E. Fog computing architecture

Fog computing architecture plays a critical role in enhancing the efficiency and effectiveness of anti-counterfeiting efforts within the pharmaceutical supply chain. By deploying fog computing at strategic points along the supply chain, local data processing becomes possible, enabling real-time analysis of data collected by IoT devices. This localized processing

capability allows for immediate detection of anomalies and deviations from predefined parameters, such as temperature thresholds or shipment routes. As the first line of defense, fog computing architecture acts swiftly to identify potential threats to medication integrity, such as fluctuations in storage conditions or unauthorized alterations in the shipment's trajectory. By providing proactive monitoring and analysis capabilities, fog computing ensures that pharmaceutical products remain safeguarded throughout their journey, thereby bolstering the overall security and reliability of the supply chain against counterfeit drugs and related risks.

Strategically positioned fog nodes in the supply chain can analyze data from IoT devices, detecting anomalies like temperature changes or route deviations in real-time. These nodes act as local hubs, processing IoT data to protect medication integrity. Amid warehouses and transit routes, they sift through data, like vigilant sentinels, to identify potential issues. With their computing power, fog nodes actively safeguard the pharmaceutical supply chain by analyzing data and alerting stakeholders to risks promptly. Blockchain technology further enhances security by ensuring data integrity and transparency throughout the supply chain, ensuring safe delivery for their life-saving purpose.

VI. PROPOSED FRAMEWORK

In this section the proposed robust and comprehensive approach to address the challenges of counterfeit pharmaceuticals in the supply chain. This system combines Blockchain and IoT technologies to enhance medication security, real-time temperature monitoring, and comprehensive tracking of pharmaceutical products. The key components of the solution include IoT sensors for temperature monitoring, Blockchain for secure data storage, smart contracts for process automation, QR code integration, and the implementation of fog computing architecture for local data processing.

A. Architecture

The system is built on a hybrid architecture combining blockchain and IoT components. Blockchain nodes are distributed across the pharmaceutical supply chain, including manufacturers, distributors, and pharmacies. IoT devices, equipped with temperature sensors and unique identifiers, are attached to individual medicine packages. These devices communicate with the blockchain network to record and verify transactions.

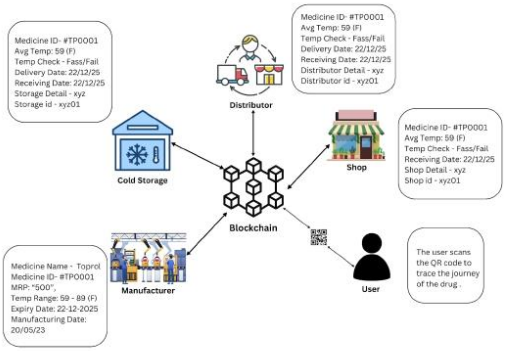

Fig. 1 Blockchain Architecture

B. Blockchain Implementation

A permissioned blockchain is employed to ensure data integrity and confidentiality among authorized participants. Smart contracts govern the rules for recording transactions and verifying the authenticity of medicines. Each transaction, representing a key event in the pharmaceutical supply chain, is cryptographically hashed and added to the blockchain, creating an immutable and transparent ledger.

Using a permissioned blockchain for this anti-counterfeiting system offers many advantages over a traditional permissionless blockchain. By restricting access to only authorized users, blockchain permissions enhance data privacy and confidentiality, reducing the risk of sensitive information being released to unauthorized parties so This access controlled system ensures that only accredited companies, such as pharmaceutical companies, distributors and only law enforcement agencies , allowing blockchain enabled effective consensus mechanism is, because network participants are known entities, which allows for faster transaction processing and scalability

Smart contracts play an important role in automating and embedding the business logic that governs the dispensing of medicines on the blockchain. These practical agreements contain fixed terms and conditions that are automatically applied when triggering events occur. In the context of anti-counterfeiting, smart contracts have been developed to authenticate medicines based on predefined criteria, such as checking the manufacturer's digital signature so, confirms the accuracy of the product sequence information -Reduces the risk of errors or changes, thereby increasing the efficiency of the overall anti-counterfeiting system and they are reliable.

C. IoT Devices

The IoT devices are embedded with temperature sensors to monitor the environmental conditions in which medicines are stored and transported. These devices are equipped with RFID

or NFC technology for unique identification. Data collected by the IoT devices, including temperature readings and location information, are securely transmitted to the blockchain for real-time recording. The implementation of IoT devices with temperature sensors marks a significant leap forward in ensuring the integrity and safety of medicinal products throughout the supply chain. Imagine these devices as vigilant guardians, constantly monitoring the environment where medicines are housed and moved. With their temperature-sensing capabilities, they act as sensitive thermometers, meticulously tracking any fluctuations that could potentially compromise the effectiveness of medications. Whether stored in a warehouse or in transit, these IoT devices stand sentinel, providing invaluable insights into the conditions that directly impact the quality of pharmaceuticals.

Moreover, these IoT devices are not just passive observers; they're equipped with cutting-edge RFID or NFC technology, akin to unique identification badges. This enables seamless tracking and tracing of each individual medicine packet or batch as it journeys from manufacturer to distributor to pharmacy. It's akin to giving each medicine its own digital identity, ensuring its authenticity and enabling quick verification at any point in the supply chain. As these IoT-enabled devices accompany medicines on their odyssey, they diligently record vital information such as temperature readings and location data, acting as faithful scribes meticulously documenting every step of the journey. This treasure trove of data is securely transmitted to the blockchain, where it is etched into the immutable ledger in real-time, providing stakeholders with unparalleled visibility and assurance regarding the integrity of the pharmaceutical supply chain.

D. Temperature Monitoring

The real-time temperature monitoring provided by the IoT devices ensures that pharmaceutical products are stored and transported within specified temperature ranges. Deviations from these ranges trigger alerts and are recorded on the blockchain, providing a transparent history of the temperature conditions throughout the product's journey.These devices serve as the ever-watchful eyes, ensuring that medicines are cocooned within the optimal temperature ranges essential for maintaining their efficacy and safety. Whether nestled in a warehouse awaiting distribution or embarking on a cross-country journey, these IoT guardians remain steadfast, continuously relaying temperature readings in real-time. In the event of any deviation from the specified temperature ranges, akin to a subtle alarm sounding in the silence, alerts are promptly triggered, signaling potential risks to the integrity of the medications.

The transparency provided by real-time temperature monitoring extends far beyond mere surveillance; it paints a vivid picture of the journey undertaken by pharmaceutical products, capturing every twist and turn in their environmental conditions. Each fluctuation in temperature, whether a fleeting spike or a prolonged dip, is meticulously recorded on the blockchain, leaving an indelible trail of the product's temperature history. This transparent chronicle not only provides stakeholders with invaluable insights into the conditions experienced by the medications but also serves as a testament to the unwavering commitment to quality and safety throughout the supply chain. By harnessing the power of real-time temperature monitoring, the anti-counterfeiting initiative not only safeguards the integrity of pharmaceutical products but also fosters a culture of accountability and trust within the industry.

E. Fog Nodes for Local Data Processing

Fog nodes placed at strategic points within the supply chain can process the data collected by IoT devices. They can perform real-time analysis to detect anomalies, such as unexpected temperature fluctuations or deviations in the shipment's route.These nodes serve as local hubs for processing the wealth of data collected by IoT devices, acting as the first line of defense against potential threats to medication integrity. Nestled amidst the bustling activity of warehouses, distribution centers, and transit routes, these nodes are poised to sift through the deluge of information pouring in from the IoT sensors. Their role is akin to vigilant sentinels, tirelessly scanning for any signs of trouble lurking within the data streams.

With their formidable computing power and analytical prowess, fog nodes are not just passive bystanders; they're active participants in safeguarding the pharmaceutical supply chain. As the guardians of local data processing, they possess the capability to perform real-time analysis, swiftly identifying anomalies that could signal trouble. Whether it's a sudden spike in temperature or an unexpected deviation in the shipment's intended path, these nodes stand ready to sound the alarm, alerting stakeholders to potential risks before they escalate. By acting as the eyes and ears of the supply chain, fog nodes play a crucial role in maintaining the integrity and security of medicinal products, ensuring that they reach their destinations unscathed and ready to fulfill their life-saving purpose.

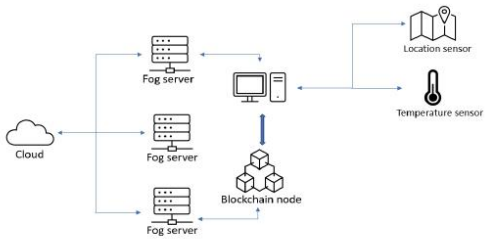

Fig. 2 Fog Architecture

F. Verification at Each Node

As the medical products move through the supply chain, each node (e.g., distributors, and pharmacies) can verify the authenticity of the products by checking their digital signatures against the blockchain records. Any discrepancy or counterfeit product can be immediately flagged for further investigation.

This verification process at each node within the supply chain not only ensures the authenticity of the medical products but also promotes accountability among stakeholders. Distributors and pharmacies can verify the legitimacy of the products they receive by cross-referencing digital signatures with blockchain records, thereby reducing the risk of inadvertently distributing counterfeit or substandard medication. Moreover, the transparency provided by blockchain technology fosters trust and collaboration among supply chain participants, as they can collectively monitor the movement of products and collaborate to address any issues or discrepancies encountered.

In addition to enhancing product authentication, the integration of blockchain and IoT enables comprehensive track-and-trace capabilities throughout the supply chain. By leveraging IoT devices such as GPS trackers and temperature sensors, stakeholders can monitor the location, condition, and handling of medical products in real time. This granular level of visibility not only helps in identifying potential points of vulnerability or diversion but also facilitates efficient recall processes in the event of quality issues or safety concerns. As a result, the implementation of blockchain and IoT technologies not only strengthens anti-counterfeiting efforts but also enhances overall supply chain management, leading to improved efficiency, safety, and consumer confidence in the pharmaceutical industry.

G. Data Security and Privacy

The use of encryption techniques and access controls ensures the security and privacy of sensitive data within the blockchain. Only authorized parties have access to specific information, maintaining confidentiality while allowing transparency within the supply chain.Within the blockchain-based anti-counterfeiting system, robust encryption techniques stand as the first line of defense against unauthorized access and malicious attacks. Picture encryption as an impenetrable fortress surrounding the data, rendering it unreadable to anyone without the proper decryption keys. This ensures that even if unauthorized parties were to gain access to the blockchain, they would be met with an insurmountable barrier, unable to decipher the encrypted information contained within.

Furthermore, access controls serve as the gatekeepers of the blockchain, carefully regulating who can view and interact with specific data. Just like a well-guarded vault, only authorized parties possess the keys to unlock access to particular information, ensuring that sensitive data remains confidential and secure. However, this doesn't mean sacrificing transparency within the supply chain; instead, it strikes a delicate balance between confidentiality and accountability. Authorized stakeholders are granted access to the information relevant to their role in the supply chain, fostering trust and collaboration while safeguarding against potential breaches of privacy. By employing encryption techniques and access controls,the blockchain-based anti-counterfeiting system not only fortifies the security of sensitive data but also upholds the privacy rights of all stakeholders involved.

H. Methodology for Proposed Work

The project employs a structural design approach to architect the system. The structural approach focuses on organizing the system's components and their interactions logically and efficiently. This approach allows us to ensure that the various elements of the system work together seamlessly to achieve the intended objectives. It involves designing the system's architecture, defining data structures, and specifying the functions and responsibilities of each component.

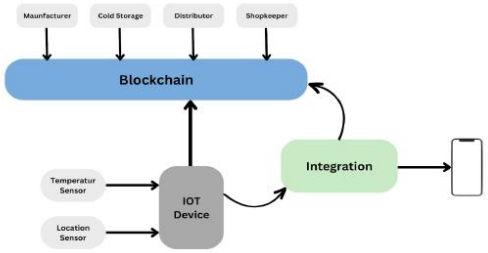

Fig. 3 System Design

VII. NOVELITY

The integration of blockchain and IoT technologies in the realm of anti-counterfeiting for medicine represents a novel and unique approach that holds immense promise. This research topic stands out for its innovative combination of two cutting-edge technologies to address a critical global issue. Blockchain's decentralized and immutable ledger provides a secure and transparent platform for tracking the entire lifecycle of pharmaceutical products, from manufacturing to consumption. IoT devices, on the other hand, enable real-time monitoring and data collection, enhancing the traceability and authenticity of medicines. Together, these technologies offer a comprehensive solution to combat the pervasive issue of counterfeit drugs, ensuring the safety and efficacy of medication for consumers worldwide. This research not only contributes to the advancement of technology but also has significant implications for public health and safety, making it a compelling and impactful area of study.

VIII. CONCLUSION

In conclusion, The utilization of Blockchain technology in conjunction with the Internet of Things (IoT) presents a promising solution to combat the pervasive issue of counterfeit medicines. Through the seamless integration of these innovative technologies, the pharmaceutical industry can revolutionize supply chain management, enhance transparency, and safeguard public health.

Blockchain's immutable and decentralized ledger system ensures the integrity and traceability of pharmaceutical products at every stage of the supply chain. By recording transactions in a tamper-resistant manner, blockchain technology provides a reliable mechanism for verifying the authenticity of medicines, thereby mitigating the risks associated with counterfeit drugs entering the market.

The integration of IoT devices such as smart tags, sensors, and RFID chips facilitates real-time monitoring and data collection throughout the entire lifecycle of pharmaceutical products. These IoT-enabled devices enable stakeholders to track the movement, storage conditions, and authenticity of medicines, thus enabling rapid detection and response to any anomalies or discrepancies.

By leveraging blockchain and IoT technologies, stakeholders can establish a transparent and auditable record of each medicine's journey from production to consumption. This enhanced visibility not only deters counterfeiters but also enables authorities to identify and intercept counterfeit products before they reach consumers.

The implementation of blockchain and IoT-based anti-counterfeiting solutions fosters collaboration among stakeholders, including manufacturers, distributors, regulators, and consumers. By sharing authenticated data in a secure and interoperable manner, stakeholders can work together to ensure the safety, efficacy, and quality of medicines worldwide.

IX. FUTURE SCOPE

The future scope section delves into the vast possibilities for advancing anti-counterfeiting efforts using blockchain and IoT. It discusses the integration of artificial intelligence (AI) and machine learning algorithms as a key area of development. These technologies have the potential to significantly improve the detection of counterfeit drugs by analyzing large datasets and identifying fraudulent patterns. Furthermore, advancements in IoT sensor technology could lead to more sophisticated tracking devices capable of providing real-time information about the location and condition of pharmaceutical products. The section also explores the potential for the widespread adoption of blockchain and IoT technologies in creating a global, interoperable network for tracking and authenticating medicines. It emphasizes the role of such a network in ensuring the safety and effectiveness of medications for patients worldwide.

A. Integration of AI and Machine Learning

The integration of AI and machine learning algorithms with blockchain and IoT systems offers promising opportunities for enhancing anti-counterfeiting efforts. These technologies can analyze vast amounts of data to detect patterns indicative of counterfeit activities, enabling proactive measures to be taken to safeguard medication authenticity. For example, AI algorithms can analyze supply chain data to identify discrepancies or anomalies that may signal the presence of counterfeit drugs.

B. Advancements in IoT Sensor Technology

Future developments in IoT sensor technology hold great potential for improving the tracking and monitoring of pharmaceutical products. Advanced sensors could provide real-time information about the location and condition of medicines, enabling stakeholders to ensure that medications remain within safe storage conditions throughout the supply chain. For instance, sensors could monitor humidity, and other environmental factors to prevent the degradation of pharmaceutical products.

C. Creation of a Global Network

The widespread adoption of blockchain and IoT technologies in the pharmaceutical industry could lead to the creation of a global, interoperable network for tracking and authenticating medicines. Such a network would enable seamless communication and data sharing among stakeholders, facilitating the traceability of medications from production to consumption. By leveraging blockchain's immutable and transparent nature, the network could establish a trustworthy record of each medication's journey, enhancing supply chain security and mitigating the risk of counterfeit drugs entering the market.

REFERENCES

[1] Shankar D. Nawale , Rahul R. Konapure Blockchain & IoT based Drugs Traceability for Pharma Industry , 01 November 2021

[2] Keshav kaushik , Shubham tayal , Susheela Dahiya Sustainable and Advanced applications of block chain in smart computational technologies, 2019

[3] Pranav Ratta, Amanpreet Kaur, Sparsh Sharma, Mohammad Shabaz, and Gaurav Dhiman Application of Blockchain and Internet of Things in Healthcare and Medical Sector: Applications, Challenges, and Future Perspectives , 25 May 2021

[4] Faisal Jamil, Lei Hang, KyuHyung Kim, DoHyeun Kim A Novel Medical Blockchain Model for Drug Supply Chain Integrity Management in a Smart Hospital, 7 May 2019

[5] Gabriella M.Hastig, Manmohan S.Sodhi Blockchain for Supply Chain Traceability: Business Requirements and Critical Success Factors, November 2019

[6] Iyolita Islam, Muhammad Nazrul Islam A blockchain based medicine production and distribution framework to prevent medicine counterfeit, January 2024

[7] Rajani Singh, Ashutosh Dhar Dwivedi, Gautam Srivastava Internet of Things Based Blockchain for Temperature Monitoring and Counterfeit Pharmaceutical Prevention, 16 July 2020

[8] Huma Saeed, Hassaan Malik, Umair Bashir, Aiesha Ahmad Blockchain technology in healthcare: A systematic review, April 2022

[9] M. Madhu Rani, A. Jawahar Traceability of Pharmaceutical Products using Blockchain, November 2023

[10] Rizwan Manzoor, B. S. Sahay & Sujeet Kumar Singh Block chain technology in supply chain management: an organizational theoretical overview and research agenda, 24 Nov 2022

[11] Vishwesh Lingayat, Isha Pardikar, Shubham Yewalekar, Shyamal Khachane Securing Pharmaceutical Supply Chain using Blockchain Technology, January 2021

[12] Chin-Ling Chen, Long-Hui Guo, Ming Zhou, Woei-Jiunn Tsaur, Hongyu Sun, Wanbing Zhan, Yong-Yuan Deng, Chun-Ta Li Blockchain-Based Anti-Counterfeiting Management System for Traceable Luxury Products, 08 October 2022

[13] Mohamed Tahar Hammi, Badis Hammi, Patrick Bellot, Ahmed Serhrouchni Bubbles of Trust: A decentralized blockchain-based authentication system for IoT, September 2018

[14] Sarmistha Sarna Gomasta, Aditi Dhali, Tahlil Tahlil, Md. Musfique Anwar, A.B. M Shawkat Ali PharmaChain: Blockchain-based drug supply chain provenance verification system, 7, July 2023

[15] Pham Hoai Luan, Thi Hong Tran, Yasuhiko Nakashima Practical Anti-Counterfeit Medicine Management System Based on Blockchain Technology, December 2019

References

[1] Shankar D. Nawale , Rahul R. Konapure Blockchain & IoT based Drugs Traceability for Pharma Industry , 01 November 2021

[2] Keshav Kaushik , Shubham tayal , Susheela Dahiya Sustainable and Advanced applications of block chain in smart computational technologies, 2019

[3] Pranav Ratta, Amanpreet Kaur, Sparsh Sharma, Mohammad Shabaz, and Gaurav Dhiman Application of Blockchain and Internet of Things in Healthcare and Medical Sector: Applications, Challenges, and Future Perspectives , 25 May 2021

[4] Faisal Jamil, Lei Hang, KyuHyung Kim, DoHyeun Kim A Novel Medical Blockchain Model for Drug Supply Chain Integrity Management in a Smart Hospital, 7 May 2019

[5] Gabriella M.Hastig, Manmohan S.Sodhi Blockchain for Supply Chain Traceability: Business Requirements and Critical Success Factors, November 2019

[6] Iyolita Islam, Muhammad Nazrul Islam A blockchain based medicine production and distribution framework to prevent medicine counterfeit, January 2024

[7] Rajani Singh, Ashutosh Dhar Dwivedi, Gautam Srivastava Internet of Things Based Blockchain for Temperature Monitoring and Counterfeit Pharmaceutical Prevention, 16 July 2020

[8] Huma Saeed, Hassaan Malik, Umair Bashir, Aiesha Ahmad Blockchain technology in healthcare: A systematic review, April 2022

[9] M. Madhu Rani, A. Jawahar Traceability of Pharmaceutical Products using Blockchain, November 2023

[10] Rizwan Manzoor, B. S. Sahay & Sujeet Kumar Singh Block chain technology in supply chain management: an organizational theoretical overview and research agenda, 24 Nov 2022

[11] Vishwesh Lingayat, Isha Pardikar, Shubham Yewalekar, Shyamal Khachane Securing Pharmaceutical Supply Chain using Blockchain Technology, January 2021

[12] Chin-Ling Chen, Long-Hui Guo, Ming Zhou, Woei-Jiunn Tsaur, Hongyu Sun, Wanbing Zhan, Yong-Yuan Deng, Chun-Ta Li Blockchain-Based Anti-Counterfeiting Management System for Traceable Luxury Products, 08 October 2022

[13] Mohamed Tahar Hammi, Badis Hammi, Patrick Bellot, Ahmed Serhrouchni Bubbles of Trust: A decentralized blockchain-based authentication system for IoT, September 2018

[14] Sarmistha Sarna Gomasta, Aditi Dhali, Tahlil Tahlil, Md. Musfique Anwar, A.B. M Shawkat Ali PharmaChain: Blockchain-based drug supply chain provenance verification system, 7, July 2023

[15] Pham Hoai Luan, Thi Hong Tran, Yasuhiko Nakashima Practical Anti-Counterfeit Medicine Management System Based on Blockchain Technology, December 2019