ENHANCING PHARMACEUTICAL SECURITY: INTEGRATING IBCDS WITH ONION ENCRYPTION

PONNADA NAGA RAMYA[1], DR. I. RAVI PRAKASH REDDY[2] and DR. SUPREETHI KP[3]

[1]Assistant Professor, Department of Information Technology, G. Narayanamma Institute of Technology and Science (For Women), Hyderabad, India.

[2]Professor&Dean, Department of IT Information Technology, G. Narayanamma Institute of Technology and Science (For Women), Hyderabad, India.

[3]Professor, Department of CSE, JNTUH UCEST, Hyderabad, India

E-mail: [1]ramyapn1.phd@gmail.com, [2]irpreddy@gnits.ac.in, [3]supreethi.pujari@jntuh.ac.in

ABSTRACT

The pharmaceutical business must rigorously strengthen its security procedures in an era marked by increasing digitization and the enduring danger of cyberattacks. According to estimates, up to 30 percent of medical products offered in underdeveloped nations are fake. This research offers a novel approach to improving pharmaceutical security through the seamless integration of two strong security technologies: Onion Encryption and Intelligent Blockchain-Based Cryptographic Data Security (IBCDS). The pharmaceutical industry operates in a cybersecurity environment that is becoming more dynamic and changing as it is tasked with protecting a variety of sensitive data, including patient information, confidential research, and priceless intellectual property. IBCDS, which is recognised for being decentralised and tamper-resistant, provides a strong basis for protecting pharmaceutical data against intrusion and alteration. Parallel to this Onion Encryption, which takes its cues from the principles of the Tor network, provides a further layer of security by obscuring data paths and guaranteeing strict secrecy. This research offers a comprehensive and integrated security approach to improve the pharmaceutical industry's overall security posture, foster stakeholder trust, and erect an impregnable fortress against the dangers of an increasingly interconnected and vulnerable digital landscape. The proposed approach gives customers the ability to independently confirm the legitimacy of medical supplies thanks to an intuitive web interface that allows for real-time product tracking via scanned QR codes. It does this through meticulous exploration of the theoretical underpinnings of these technologies and empirical validation of their efficacy via existing literature and practical case studies.

Keywords: *Pharmaceutical Security, Blockchain technology, Cryptographic Data Security, onion encryption, Data protection*

1. INTRODUCTION

The pharmaceutical sector is not exempt from the urgent issues of data security and integrity at a time of fast technological advancement. It has proven to be a difficult challenge to guarantee both privacy and traceability in pharmaceutical transactions, and existing solutions are frequently confined in their use. This study sets out on a quest to offer a thorough and all-encompassing solution that incorporates the ground-breaking idea of Onion chain. Onion chain provides a set of protocols intended to make privacy-preserving and traceable transactions within the pharmaceutical industry possible by drawing inspiration from the concepts of onion routing [11]. These protocols cover the key phases of sign-up, message transmission, and identity revelation, all of which operate without a hitch within the constraints of blockchain technology. Parties taking part in Onion chain are required under the registration protocol to reveal their genuine identities, which are subsequently disseminated and safely preserved on the blockchain and open to the public [2]. The privacy of all parties involved is protected despite this accessibility because to our architecture, which makes sure that even with public access, malevolent actors cannot link particular messages to their senders.

The message transmission protocol reimagines how parties communicate by demanding that data be recorded on the blockchain as encrypted proof using mutually agreed-upon keys. When circumstances call for disclosure, such as the discovery of misleading information, this proof, which is essential to the identity disclosure protocol, is crucial in revealing the sender. In these circumstances, our identity revelation approach successfully uses the stored evidence's decryption to link false information to a particular sender [12]. We examine Onion chain's protocols in further detail in the following sections and make a case for their adoption by the pharmaceutical sector. We demonstrate its robustness and efficacy through in-depth security study and experimentation. Our research ushers in a new age where privacy, traceability, and data integrity coexist peacefully inside a blockchain-based framework, marking a substantial leap in pharmaceutical security [4].

The pharmaceutical sector, which is devoted to the research and distribution of life-saving drugs and cures, is a crucial pillar of contemporary healthcare. However, as the pharmaceutical industry develops and digitises further, it becomes more open to cyber-attacks, data breaches, and the introduction of substandard medications [13]. From research and development through production and distribution, protecting sensitive pharmaceutical data is essential for protecting intellectual property as well as the safety and effectiveness of pharmaceuticals. This research study looks into the world of advanced data security technologies to solve these urgent issues, and it suggests a revolutionary strategy that combines the strength of onion encryption with the intelligence of blockchain-based intelligent cryptographic data security [14]. By combining these two cutting-edge technologies, we want to strengthen the data protection measures used by the pharmaceutical industry, promoting confidence, security, and integrity along the whole pharmaceutical supply chain. In this essay, we'll look at the complicated problems that the pharmaceutical business has to deal with when it comes to safeguarding confidential information both within and across various stakeholder organisations [7]. We will also go into the flaws that standard data security solutions have, emphasising the necessity for creative ways to counter new dangers. Our system creates a secure basis for pharmaceutical data by utilising the decentralised and unchangeable properties of blockchain technology. Data authenticity and integrity are guaranteed at every stage of the pharmaceutical lifecycle, from research and clinical trials through manufacturing and distribution, through the integration of intelligent blockchain-based cryptographic data protection.

To complement this, we present an onion encryption scheme that gives the data secured by blockchain an extra layer of protection. This sophisticated encryption technique adds an unheard-of level of secrecy and anonymity to the data by guaranteeing that only authorised people may access and decode important pharmaceutical information. We will thoroughly examine the fundamentals of onion encryption, blockchain technology, and cryptographic data security throughout this research paper to show how these elements combine to fortify the pharmaceutical industry's data protection with an impregnable fortress. In order to demonstrate the viability and benefits of our suggested approach, we will also provide real-world case studies and examples of actual implementations [8]. As a result, our study makes a significant addition to efforts being made to improve pharmaceutical security. We aim to provide pharmaceutical organisations with the tools they need to safeguard their priceless data assets, protect the integrity of medications, and ultimately ensure the wellbeing of patients around the world by combining intelligent blockchain-based cryptographic data security with onion encryption.

Revolutionizing Healthcare Supply Chain Tracking with Innovative Technologies.

The typical healthcare supply chain is described with Partners in figure 1 below. Barcode technology, Radio Frequency Identification (RFID), and Electronic Product Code (EPC) have long been used by conventional supply chain services to track and control commodities as they move through the supply chain. These technologies 135 enable the use of Global Standards 1 (GS1) standards barcodes to record and communicate product data, such as unique serial numbers, manufacturing dates, and expiration dates. RFID tags are scalable and data-storing devices, but they may be costly to install and may not work well in situations where radio frequency waves clash or are blocked [15]. By generating a Data-Matrix with details for every medication, the utilization of a Data-Matrix monitoring system further improves traceability. for example, the product ID, producer ID, package ID, and more metadata. However, compared to Quick Response (QR) scans, data matrix codes can only retain a finite amount of information.

The supply chain process for pharmaceuticals, or medical items, from manufacture to distribution and sale, is depicted in the figure 2 using blockchain technology. There are several steps in the process: manufacturing, regulation, distribution, transportation, monitoring, and sale. Transparency, security, and efficiency are ensured in the supply chain process by using smart contracts and blockchain technology to automate and simplify it. By lowering mistakes and minimizing fraud, the usage of QR codes aids in confirming the legitimacy of medical supplies [16]. To ensure the patients' health and safety, the procedure encompasses customers, distributors, merchants, logistics units, and regulatory organizations. The blockchain is used to store the data created during the supply chain process, giving rise to an impenetrable transaction record.

This study focuses on the critical need for improved security measures in the pharmaceutical business, as rising cyber threats and counterfeit hazards represent substantial problems. By using modern security technologies such as Onion Encryption and IBCDS, the study hopes to address a major vacuum in the current literature by presenting a complete security framework customized particularly to the pharmaceutical industry's unique demands. This integrated strategy not only improves industry security, but it also gives stakeholders the ability to independently verify product authenticity, encouraging trust and confidence.

Problem Statement

The pharmaceutical business confronts increasing cyber threats and counterfeit product dangers, with up to 30% of medicinal goods faked in developing countries.

Research attempts to increase pharmaceutical security by merging Onion Encryption with IBCDS.

IBCDS provides decentralized, tamper-resistant protection for pharmaceutical data, which is enhanced by Onion Encryption's data route obfuscation and secrecy protections.

The proposed strategy improves overall industry security, builds stakeholder confidence, and protects against emerging cyber threats.

Customers are enabled to check the reliability of medical supplies using a simple online interface and QR code tracking.

Research based on fundamental theories and validated by literature reviews and practical case studies.

2. LITERATURE REVIEW

The literature study includes significant contributions to research in the fields of mobile ad hoc networks (MANETs), blockchain technology, the Internet of Things (IoT), and very high-speed very large-scale integration (VHV) channel routing. Research in MANETs focuses on resource-constrained node energy-efficient routing to improve network dependability. Integrating a blockchain with homomorphic encryption improves data security by guaranteeing its integrity and confidentiality. Blockchain and smart contracts are used in IoT research to provide open, safe access control systems, reducing security issues. Combining encryption with blockchain-based cryptographic data security in the pharmaceutical industry improves data protection and secures pharmaceutical information. Advanced routing methods in Vehicular Ad-Hoc Networks (VANETs) increase communication reliability while optimising data delivery and neighbour recognition accuracy in dynamic VANET topologies. Together, these scientific contributions improve the security, effectiveness, and dependability of these technologies, having significant effects on several different businesses.

Due to node mobility and dynamic conditions, MANETs (Mobile ad hoc networks) have routing difficulties. A flexible adaptive multipath routing technology that supports many applications was put forth by Akshay Parihar et al. [1]. It prioritises security, optimises data speeds for multimedia, and leverages conventional on-demand routing for simplicity. Cross-layer communication improves judgement. Through rigorous simulations in various circumstances, the protocol's effectiveness and fault tolerance were proved, effectively overcoming the issues faced by MANET. Through rigorous simulations in various circumstances, the result method's effectiveness and fault tolerance were proved, effectively overcoming the issues faced by MANET. The issues of cross-domain data sharing on blockchain networks are addressed by Hang Thanh Bui et al. [3] in their research, "CD-ABSE." Their approach combines searchable encryption with attribute-based encryption to guarantee data privacy and effective keyword searches. The results reveal improved data privacy, effective searching, and interoperability with blockchains, showing the value of research in terms of safe cross-domain data exchange. In the research addressed by Muhammad Shah Ab Rahim et al. [5] tackles the difficulties in securing IoT cross-domain access control and allowing safe access rights delegation. Their method makes use of blockchain technology and smart contracts to create an extremely transparent and secure access control system, which enhances security, transparent access management, and IoT device efficiency. This research illustrates the viability as well as the effectiveness of leveraging blockchain to improve IoT access control and delegation, providing a significant response to IoT security problems. It is difficult to create routing systems for dynamic IoT networks that are effective and flexible. ensuring safe and trustworthy connection, particularly for delicate IoT data. Implementing smart contracts on the blockchain to automate and enforce routing choices while maintaining contractual obligations is described in the research of Mourad Benmalek et al. [6]. integrating this protocol into blockchain technology to benefit from its immutability and decentralisation for improved IoT routing. The protocol guarantees safe and effective IoT routing, upholding data confidentiality and integrity while lowering latency and enhancing overall IoT communication dependability. A significant difficulty is effectively managing energy resources in the Industrial Internet of Things (IIoT) to increase device lifespans and lower operational expenses. It is essential to provide safe and reliable data transfer in the IIoT, especially when handling sensitive industrial data. In this research, [9] Darin Mansor Mathkor et al. [9] proposed an "Energy-Aware Routing Protocol with Fuzzy Logic in IIoT with Blockchain Technology." Key techniques include Utilising fuzzy logic for dynamic routing decisions to improve IIoT network performance and energy consumption and enhancing data security, immutability, and transparency in IIoT data transfers by using blockchain technology. By optimising energy usage, the protocol successfully increases the lifespans of IIoT devices. Blockchain integration guarantees safe and impenetrable data transfer, upholding data integrity and sustaining user confidence in IIoT applications.

In mobile ad hoc networks (MANETs) with resource-constrained nodes, it is critical to control energy usage at the MAC (Medium Access Control) layer. Due to the constant and erratic topology changes in MANETs, optimising routing methods is challenging. Techniques to reduce MAC layer power consumption, lengthen node lifetime, and algorithms to increase routing protocol efficiency, boosting route discovery and maintenance in dynamic MANETs were developed by Bruno Ramos-Cruz et al. [10]. By consuming less energy, the suggested MAC optimisations increase node lifespans. The optimisation approach boosts the speed of the routing protocol, facilitating effective route management in dynamic MANET environments. In order to promote network dependability, our study improves both energy efficiency and the efficacy of the routing protocol. It can be challenging to guarantee the security and confidentiality of data communicated via a blockchain network, especially when working with sensitive material. Homomorphic encryption can be used in a blockchain environment to provide safe data transmission while protecting privacy. Kannan Govindan et al. [21] tackles the challenges in this research using homomorphic encryption techniques to enable calculations on encrypted data without disclosing the underlying data and integrating this secure data transmission method into a blockchain network to improve data confidentiality and integrity during transmission. The proposed approach guarantees secure data transfer via a blockchain network, safeguarding it from unauthorised access and preserving confidentiality. Homomorphic encryption protects secrecy during data transmission and enables calculations on encrypted data without jeopardising privacy. Due to the continually shifting locations of the cars, accurately recognising nearby vehicles with directional antennas in dynamic Vehicular Ad-Hoc Networks (VANETs) is difficult. It is difficult yet crucial to create effective routing protocols that can change to the dynamic VANET architecture with directional antennas. In this research, Sotirios Messinis Li et al. [22] proposed a "Routing Protocol in VANETs Equipped with Directional Antennas." Designing a system for precise neighbour identification, taking into account VANETs' dynamic nature, and assessing the effectiveness of routing methods in directional antenna settings to guarantee effective data delivery. The suggested strategy improves communication reliability in VANETs with directional antennas by enhancing neighbour identification precision. Data transfer is effective and communication lags are minimised due to the research of routing algorithms, which guarantees flexibility to dynamic VANET topologies. In vehicle networks using directional antennas, our approach improves communication efficiency and dependability. It can be difficult to strike a balance between privacy and traceability in blockchain transactions since conventional blockchain systems frequently reveal transaction information to all users. The research by Hai Ziwei et al. [23] describes the use of group signature techniques to permit transaction anonymity while maintaining the ability to track activities back to particular groups when necessary are important strategies. incorporating this protocol with blockchain technology to improve transaction privacy and traceability. By guaranteeing transaction anonymity within the blockchain, the proposed protocol safeguards user privacy. Even though transactions are anonymous, the protocol permits tracing when necessary, boosting the security and reliability of blockchain applications. It is difficult to properly route signals in a three-layer Very High-Speed Very Large-Scale Integration (VHV) channel because crosstalk must be minimised while resource use must be optimised. For three-layer VHV channel routing, the research by Fatima Alwahedi et al. [24] introduces the approach which include the three-layer VHV channel requires the development of algorithms and tactics to limit crosstalk between signals, which is crucial for signal integrity and vertically assigning routing channels will maximise the use of the available layers while reducing crosstalk. Signal dependability is increased by the suggested method's efficient minimization of crosstalk in three-layer VHV channel routing. The strategy improves overall efficiency by optimising resource utilisation in the VHV channel by allocating routing pathways vertically.

Earlier research outlined issues with MANETs, blockchain, IoT, IIoT, VANETs, and VHV channel routing. These problems included interference in VHV channel routing, data privacy in blockchains, sophisticated IoT access control, energy management in IIoT, and routing efficiency in MANETs with directional antennas. However, future studies aim to overcome these difficulties using cutting-edge techniques. The solutions suggested include energy-efficient IIoT routing integrated with blockchain, adaptive multipath routing for MANETs, advanced data privacy techniques for blockchain, transparent IoT access control via blockchain and smart contracts, enhanced routing in VANETs with directional antennas, and crosstalk mitigation in VHV channel routing. These next techniques show promise for enhancing the reliability, efficiency, and security of these crucial technologies while overcoming persistent challenges identified in earlier studies.

Key Findings

- A proposed adaptive multipath routing technology effectively addresses routing challenges in Mobile Ad hoc Networks (MANETs), enhancing network reliability through simulations.
- The CD-ABSE protocol resolves cross-domain data sharing issues on blockchain networks, ensuring data privacy and enabling effective keyword searches.
- Leveraging blockchain technology for IoT access control provides transparency and security, enhancing trust in IoT ecosystems.
- Smart contracts automate and enforce routing decisions in dynamic IoT networks, ensuring secure and reliable connections.
- Energy-aware routing protocols in Industrial Internet of Things (IIoT) with blockchain optimize energy usage, prolonging device lifespans and enhancing data security.
- Techniques to reduce MAC layer power consumption in MANETs improve energy efficiency and routing protocol effectiveness, enhancing network performance.
- Homomorphic encryption safeguards data confidentiality and integrity in blockchain networks, ensuring secure data transmission.

3. METHODOLOGY

The initiative Medical Counterfeit aims to tackle the widespread problem of fake medical items in supply chains by combining many technologies such as blockchain, Remix IDE, Ganache, MetaMask, JavaScript, PHP, XAMPP, and Onion routing. The project takes a multi-pronged strategy, starting with the definition of discrete entity roles as retailer, distributor, manufacturer, and consumer. The only people who can add products to the blockchain are manufacturers, therefore the system's integrity is guaranteed. JavaScript features for QR code creation and scanning enable each product to be given a unique ID and QR code for effective tracking throughout the supply chain [17]. XAMPP offers a complete local database management solution, and is used to securely store data related to manufacturers, distributors, retailers, and consumers.

To ensure smooth data administration and retrieval, data such as user profiles, product details, transaction history, and authentication credentials are stored in XAMPP's MySQL database.

Distributors, merchants, and consumers may all verify the legitimacy of products and follow their path, and blockchain querying and verification requests are supported by a PHP backend [18]. The PHP backend is hosted locally and tested using the XAMPP server, which offers a smooth development environment.

Onion routing is used to improve security and privacy by encrypting communications and protecting against hacking and monitoring across a number of relay hops. Given estimates that as much as thirty percent of medical products sold in developing countries are fraudulent, the suggested method gives consumers the ability to independently verify the authenticity of medical supplies [19]. An easy-to-use web interface makes it possible to track products in real time by scanning QR codes. Consumers may quickly verify the authenticity of medical products and feel secure about their purchases by simply accessing the web interface and scanning the QR codes on the products [20].

The project promotes security, scalability, and decentralization, building upon the Onion chain protocol. Secure message delivery is ensured via successive encryption layers, blockchain-based evidence recording, and the requirement for a majority vote to reveal a party's identity, which protects sensitive data and ensures anonymity [25]. The protocol achieves a balance between privacy and transparency by preventing the publication of illegal information, so improving the legitimacy of medical products while maintaining confidentiality.

Figure 3 shows there are several steps in the supply chain process for medical supplies, including manufacturing, packaging, shipping, and patient delivery. Using a smart contract—a self-executing agreement with stipulations encoded straight into code—the manufacturer starts production. After being packaged, the medical supplies are sent to the distributor, who scans a QR code to confirm their legitimacy [26]. Orders are sent by the distributor to the pharmacy, which scans the QR code on the items to confirm their authenticity before distributing them to patients. By scanning the QR code, patients may confirm the authenticity of medical supplies and examine the supply chain flow of the products. This procedure lowers mistakes and stops fraud by ensuring efficiency, security, and transparency in the medical supply chain. In order to preserve the validity and traceability of medical items and guarantee that patients receive real, high-quality products, smart contracts and QR code verification are used. All things considered, this procedure is critical to preserving patient health and safety as well as the integrity of the medical supply sector.

MD5 (Message Digest Algorithm 5)

Algorithm 1: - Product Submission

Initialize Parameters: Set up the necessary parameters for the product submission process.

Input: User-provided information including product ID, QR code, and description of the fake product.

Generate MD5 Hash: Apply MD5 hashing algorithm to the input data to create a unique hash.

Hash Storage:

If Hash Generation is successful:

Store Hash: Save the generated MD5 hash along with the complaint details in the blockchain for reference.

Else:

Notify Hash Failure: In case of unsuccessful hash generation, notify users of an issue in processing the complaint.

The algorithm 1 was developed to process product submissions. It requires data supplied by the user, including the product's ID, QR code, and description. The process then uses the supplied data to construct an MD5 hash, which gives the complaint a unique identify [27]. The algorithm saves the hash and the complaint data in the blockchain for later use if the hash generation process is successful. Users are notified by the algorithm if there is a problem with processing the complaint if the hash creation fails.

$$MD5(M) = \frac{MD5 - compression(MD5 - padding(M,l))}{1} \quad (1)$$

Where,
M: Input message.
MD5-padding(M,l) : Padding function for input message M with a specified length l.
MD5-compression(.): Compression function specific to the MD5 algorithm

SHA-256 (Secure Hash Algorithm 256-bit)

Algorithm 2: - Manufacturer's QR Code Scanning

Initialize Parameters: Define the parameters for the QR code scanning process during product manufacturing.

Input: Prescription received from the pharmacy and QR code generated during the manufacturing process.

Generate SHA-256 Hash: Utilize SHA-256 hashing algorithm to create a secure hash of the input data.

Compliance Check:

If Compliance Check is successful:

Record Scan Result: Store the hash and scan result in the blockchain for traceability and accountability.

Else:

Flag Non-Compliance: In case of non-compliance, flag the issue for further investigation and resolution.

The SHA-256 hashing technique is used by the Manufacturer's QR Code Scanning method to guarantee data integrity during the product making process. The prescription from the pharmacy and the QR code of the product are inputted when parameters are initialized to determine the scanning process. This data is hashed securely using SHA-256 and then put through a compliance check. Should the check be successful, indicating compliance with legal requirements, the hash and scan result are added to the blockchain, improving accountability and traceability. In contrast, the algorithm 2 detects variances from anticipated norms and identifies non-compliance for additional inquiry and resolution [28]. Strong quality control and regulatory compliance in pharmaceutical supply chains are made easier by the algorithm, which also increases stakeholder confidence and transparency.

$$SHA-256(M) = \frac{SHA-256-compression(SHA-256-padding(M,l))}{1} \qquad (2)$$

Where,

M: Input message.
SHA-256-padding(M,l) : Padding function for input message M with a specified length l.
SHA-256-compression(.): Compression function specific to the SHA-256 algorithm.
Keccak (Used in Ethereum)

Algorithm 3: - Distributor's Payment and Control

Initialize Parameters: Set up parameters for the distributor's control and payment process.

Input: Notification from the manufacturer, product delivery details, and purchase price.

Generate Keccak Hash: Apply Keccak hashing algorithm to create a unique hash for the transaction.

Hash Verification:

If Hash Verification is successful:

Distributor's Control: Assume control of the distribution procedure.

Uphold Accountability: Ensure transparency in business practices by linking the hash to the transaction.

Else:

Notify of Hash Mismatch: In case of unsuccessful hash verification, notify stakeholders of a potential issue.

Keccak hashing powers the Distributor's Payment and Control algorithm, which guarantees safe and open supply chain transactions. The algorithm 3 creates a unique hash for the transaction after it has received the notice, delivery information, and purchase price. By connecting the hash to the transaction, a successful hash verification enables the distributor to take charge of the distribution process and preserve transparency [29]. When there is a verification failure, stakeholders are alerted right away, which speeds up the inquiry and resolution process. It improves supply chain transaction security and trust.

$$Keccak(M) = \frac{Keccak-f(Keccak-padding(M,l))}{1} \quad (3)$$

Where,

Keccak(M): Keccak hash of message M

Keccak-padding(M,l) : Padding of message M for Keccak, ensuring a specified length l.

Keccak-f: Permutation function used in Keccak.

ECDSA (Elliptic Curve Digital Signature Algorithm) for Digital Signatures

Algorithm 4: - User Authentication and Access Control

Initialize Parameters: Set up parameters for user authentication and access control in the decentralized web application.

Input: User credentials (username, password), account type, and access permissions.

ECDSA Signing: Utilize ECDSA to create a digital signature for user authentication.

Signature Verification:

If Signature Verification is successful:

Direct User: Based on the account type, direct users to the appropriate pages in the personalized interface.

Else:

Deny Access: In case of unsuccessful signature verification, deny access and notify users of authentication failure.

The User Authentication and Access Control method creates a safe environment for decentralized web application access by using the Elliptic Curve Digital Signature technique (ECDSA) for digital signatures. Inputs include account type, access rights, and user credentials such passwords and usernames. Parameters are initialized to set up the authentication procedure. To create a digital signature for user authentication, ECDSA is used. The user is then sent to the relevant pages inside the tailored interface based on their account type after the algorithm 4 has successfully verified the signature [30]. Nevertheless, access is refused and users are quickly informed of the authentication failure in the event that the signature verification is failed, guaranteeing a strong and secure user authentication system in the decentralized web application.

$$ECDSA - Sign(M,d) = \frac{(r,s)}{1} \quad (4)$$

Where,

ECDSA-Sign(M,d) : ECDSA digital signature generation for message M with private key d.

(r,s): Components of the ECDSA signature.

AES (Advanced Encryption Standard) for Encryption

Algorithm 5: - Secure Data Exchange in Supply Chain

Initialize Parameters: Establish parameters for secure data exchange in the supply chain application.

Input: Data to be exchanged between stakeholders (manufacturer, distributor, pharmacy, etc.).

AES Encryption: Utilize AES for encrypting sensitive data during exchange.

Data Integrity Check:

If Data Integrity Check is successful:

Exchange Data: Allow secure data exchange among stakeholders.

Else:

Abort Exchange: In case of unsuccessful data integrity check, abort the data exchange process.

Data integrity and confidentiality are guaranteed when stakeholders exchange data using the Secure Data Exchange in Supply Chain technique, which uses the Advanced Encryption Standard (AES) for encryption. In order to create a safe data exchange, parameters are set up, and sensitive data that is exchanged by manufacturers, distributors, and pharmacies is one of the inputs. subsequently AES encryption is used to protect the data's secrecy while it is being transmitted. To confirm the integrity of the encrypted data, a data integrity check is then carried out. In the event that the check is successful and the data has been determined to be valid, stakeholders may communicate securely. To avoid unwanted access or manipulation, the algorithm stops the data sharing process if the integrity check is unsuccessful, indicating possible tampering or corruption as shown in algorithm 5.

$$AES - Encrypt(M,K) = J(AES - Round\left(AES - AddRoundKey\left(AES\ SubBytes\left(AES - ShiftRows(AES - MixColumns(M))\right), K\right)\right), 1) \tag{5}$$

Where,

AES-Encrypt(M,K): AES encryption of message M with key K

AES-Round,AES-AddRoundKey,AES SubBytes,AES-ShiftRows, AES-MixColumns : Operations used in the AES encryption algorithm.

HMAC (Hash-based Message Authentication Code) for Message Integrity

Algorithm 6: - Blockchain Transaction Verification

Initialize Parameters: Set parameters for verifying blockchain transactions related to pharmaceutical supply chain operations.

Input: Transaction details, including sender, receiver, and transaction content.

HMAC Generation: Use HMAC to generate a message authentication code for the transaction.

Integrity Verification:

If Integrity Verification is successful:

Update Blockchain: Allow the update of blockchain to reflect the transaction and maintain integrity.

Else:

Reject Transaction: In case of unsuccessful integrity verification, reject the transaction and notify stakeholders of potential tampering.

In pharmaceuticals supply chain operations, message integrity is guaranteed using the HMAC-based Blockchain Transaction Verification algorithm. It generates a unique code for transaction authentication using HMAC. Failure to verify integrity leads in transaction rejection and communication to stakeholders, protecting against possible manipulation. Success in integrity verification permits updates to the blockchain, preserving entire integrity.

$$HMAC(M,K) = H((K \oplus opad) \parallel H((K \oplus ipad) \parallel M)) \tag{6}$$

Where,

HMAC(M,K): HMAC generation for message M with key K.

H: Hash function used in HMAC.

$\oplus$: Bitwise XOR operation.

opad, ipad: Outer and inner padding used in HMAC.

4. RESULTS

The Ganache blockchain interface shows five blocks of granular data, with a focus on transaction details like gas use and timestamps; the Gas Price and Gas Limit are kept constant. An Ethereum transaction containing sender and recipient addresses, a transaction hash created by Keccak, gas settings, and information is shown in the transaction tab picture that is attached. Cryptographic methods including AES, HMAC, ECDSA, and Keccak-256 are used by Ethereum. Keccak guarantees distinct transaction IDs, facilitating safe storing via instruments such as Metamask. The fifth block details in a local Ethereum blockchain created by Ganache include a gas limit of 6,721,975, 137,441 gas consumed, and Keccak hashing for block identification, which guarantees data veracity and integrity while the network is being monitored.

The initiative's main website provides a thorough introduction, highlighting the significance of medicine safety and thwarting the sale of fake goods. It describes how the platform uses Ganache Metamask, blockchain, and onion encryption to guarantee security and openness in the tracking of medicinal supplies. Product registration, tracking, verification, security, and an intuitive user interface are among the essential aspects. In the bottom, there are connections to social networking pages, contact details, and guidelines and documentation. In general, the page promotes user participation to guarantee safe pharmaceutical practices Shows in figure 4.

While the primary content section supports product verification through input fields and QR code scanning, users may also add new items, track shipments, and check the legitimacy of products. Users can input a product ID or scan a QR code to access full product information shows in figure 5.

Figure 6 shows created QR code is displayed with the image, which shows how a medical product was successfully added to the system. A unique Product ID issued by the system—accompanies a message confirming the product's successful insertion. Users may easily view the product's details by scanning the QR code that contains its information. A prompt also recommends printing the QR code for labelling or storing in hard copy. Users can choose to go on to another area of the program or return to the previous page by clicking the "Done" button.

Figure 7 shows data for five blocks is displayed on the Ganache blockchain simulation interface, with block number five denoting the most recent block. Every block displays the amount of gas used by each individual transaction, while the Mined-on field provides the block formation timestamp. Interestingly, the Gas Price and Gas limit values stay the same for every block. It is noteworthy, though, that no explicit or direct mention of the particular hashing algorithm used for block identification is made in this context. This suggests that the interface focuses more on transaction-level information than on the complexities of block hashing algorithms.

Figure 8 shows the Ganache transaction tab, which displays information on a transaction that was completed on the local Ethereum blockchain. It contains vital transaction details like the sender and recipient addresses, the unique Transaction Hash created by the Keccak hashing algorithm, parameters related to gas like Gas Price and Gas Limit, and data specifics like the amount of transferred Ether and input data encoded with the ABI. It also includes transaction metadata that offers detailed insights into the transaction's location on the blockchain, such as Nonce, Block Hash, Block Number, and Transaction Index. The transaction was automatically mined, as shown by the Mining Status, and took place on network ID 5777, which represents the Ganache personal blockchain environment. Ethereum also uses AES for encryption, HMAC for message authentication codes, ECDSA for digital signatures, and Keccak-256 for hashing.

In a blockchain, the Keccak hashing method is used to generate distinct IDs for every transaction, guaranteeing data authenticity and integrity shown in Figure 9. Transactions are safely stored on the blockchain and made possible using the well-known bitcoin wallet browser plugin Metamask. By creating an unchangeable and visible record of medication transactions, this not only increases patient safety but also reduces the possibility of counterfeit pharmaceuticals. This technology makes the medicine supply chain traceable and verifiable, improving patient safety by ensuring the legitimacy of the drugs and lowering the frequency of fake drugs in healthcare systems.

Figure 10 shows current block number in a local Ethereum blockchain environment that is run by Ganache is 5. With a gas limit of 6,721,975, this block has used 137,441 gas. This block contains all of the transaction details, including the sender's account address, transaction hash, and gas price for each transaction. The mining state is indicated as AUTOMINING, and the network ID is 5777. and the Keccak hashing technique is used to construct the block hash, which serves as its unique identification. This thorough presentation in the Ganache blocks tab allows for effective blockchain activity monitoring while using cryptographic techniques to guarantee the validity and integrity of recorded data.

The findings reveal important information about the process of making strategic decisions, as seen by the histogram that shows the frequency of algorithms that were excluded from the proposed framework due to security and privacy concerns. Notable trends in algorithmic preferences are shown by the data; for example, algorithms like PoS and SHA-256 exhibit increased frequency of consideration for dropping, which may indicate future security standards or weaknesses. This thorough analysis of algorithmic decisions highlights how crucial it is for the framework to include strong security and privacy safeguards. In the end, it will help to improve resilience and confidence in digital systems by highlighting the need for continued research and development efforts to find substitute solutions that can handle new threats and legal requirements as shown in figure 11.

5. COMPARATIVE ANALYSIS

Table 1 displays a comparison analysis emphasizing important distinctions from the previous research study. Our research is unique in that it provides specific information on the technology used, with an emphasis on addressing the issue of fake medical supplies in the supply chain. In addition to defining entity responsibilities and addressing particular difficulties within the supply chain, both techniques go one step further by utilizing XAMPP's MySQL database to specify data storage and by including a user-friendly verification mechanism through blockchain querying and QR code scanning. Furthermore, our strategy is unique in that it prioritizes privacy and anonymity protections by utilizing Onion routing and many encryption approaches. The purpose of the research's commercial effect is to improve the medical supply chain. Interestingly, our method covers certain cryptographic algorithms, giving a thorough rundown of the methods used.

6. CONCLUSION

The integration of Onion Encryption with Intelligent Blockchain-Based Cryptographic Data Security (IBCDS) represents a significant advancement in pharmaceutical security. The pressing need for robust security measures in the pharmaceutical industry, driven by escalating cyber threats and counterfeit risks, necessitates innovative solutions. By seamlessly integrating Onion Encryption and IBCDS, our research proposes a comprehensive security framework tailored to the industry's unique challenges. This approach not only addresses the immediate concerns of data breaches and counterfeit pharmaceuticals but also prioritizes data privacy and integrity. The use of advanced encryption techniques such as Keccak, AES, HMAC, and ECDSA ensures the confidentiality and authenticity of sensitive pharmaceutical data. Furthermore, the inclusion of a user-friendly verification mechanism through blockchain querying and QR code scanning empowers stakeholders to independently verify product authenticity, fostering trust and confidence. Through a comparative analysis highlighting the distinctiveness of our approach and its emphasis on privacy measures, it is evident that our research offers a unique and effective solution to the challenges faced by the pharmaceutical supply chain. By establishing a strong defense against emerging cyber threats and cultivating stakeholder trust, our integrated security framework advances innovative techniques while safeguarding the integrity of pharmaceutical data and ensuring patient safety.

REFERENCES:

[1] Akshay Parihar, Jigna B. Prajapati, Bhupendra G. Prajapati, Binti Trambadiya, Arti Thakkar, Pinalkumar Engineer, Role of IOT in healthcare: Applications, security & privacy concerns, Intelligent Pharmacy, 2024, ISSN 2949-866X, https://doi.org/10.1016/j.ipha.2024.01.003.

[2] Nilesh Kumar Jadav, Riya Kakkar, Harsh Mankodiya, Rajesh Gupta, Sudeep Tanwar, Smita Agrawal, Ravi Sharma, GRADE: Deep learning and garlic routing-based secure data sharing framework for IIoT beyond 5G, Digital Communications and Networks, Volume 9, Issue 2, 2023, Pages 422-435, ISSN 2352-8648, https://doi.org/10.1016/j.dcan.2022.11.004.

[3] Hang Thanh Bui, Hamed Aboutorab, Arash Mahboubi, Yansong Gao, Nazatul Haque Sultan, Aufeef Chauhan, Mohammad Zavid Parvez, Michael Bewong, Rafiqul Islam, Zahid Islam, Seyit A. Camtepe, Praveen Gauravaram, Dineshkumar Singh, M. Ali Babar, Shihao Yan, Agriculture 4.0 and beyond: Evaluating cyber threat intelligence sources and techniques in smart farming ecosystems, Computers & Security, Volume 140, 2024, 103754, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2024.103754.

[4] Nhien Rust-Nguyen, Shruti Sharma, Mark Stamp, Darknet traffic classification and adversarial attacks using machine learning, Computers & Security, Volume 127, 2023, 103098, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2023.103098.

[5] Muhammad Shah Ab Rahim, Genserik Reniers, Ming Yang, Shailendra Bajpai, Risk assessment methods for process safety, process security and resilience in the chemical process industry: A thorough literature review, Journal of Loss

Prevention in the Process Industries, Volume 88, 2024, 105274, ISSN 0950-4230, https://doi.org/10.1016/j.jlp.2024.105274.

[6] Mourad Benmalek, Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges, Internet of Things and Cyber-Physical Systems, Volume 4, 2024, Pages 186-202, ISSN 2667-3452, https://doi.org/10.1016/j.iotcps.2023.12.001.

[7] Olusogo Popoola, Marcos Rodrigues, Jims Marchang, Alex Shenfield, Augustine Ikpehia, Jumoke Popoola, A critical literature review of security and privacy in smart home healthcare schemes adopting IoT & blockchain: Problems, Challenges and Solutions, Blockchain: Research and Applications, 2023, 100178, ISSN 2096-7209, https://doi.org/10.1016/j.bcra.2023.100178.

[8] Abderahman Rejeb, Karim Rejeb, Andrea Appolloni, Sandeep Jagtap, Mohammad Iranmanesh, Salem Alghamdi, Yaser Alhasawi, Yasanur Kayikci, Unleashing the power of internet of things and blockchain: A comprehensive analysis and future directions, Internet of Things and Cyber-Physical Systems, Volume 4, 2024, Pages 1-18, ISSN 2667-3452, https://doi.org/10.1016/j.iotcps.2023.06.003.

[9] Darin Mansor Mathkor, Noof Mathkor, Zaid Bassfar, Farkad Bantun, Petr Slama, Faraz Ahmad, Shafiul Haque, Multirole of the internet of medical things (IoMT) in biomedical systems for managing smart healthcare systems: An overview of current and future innovative trends, Journal of Infection and Public Health, Volume 17, Issue 4, 2024, Pages 559-572, ISSN 1876-0341, https://doi.org/10.1016/j.jiph.2024.01.013.

[10] Bruno Ramos-Cruz, Javier Andreu-Perez, Luis Martínez, The cybersecurity mesh: A comprehensive survey of involved artificial intelligence methods, cryptographic protocols and challenges for future research, Neurocomputing, 2024, 127427, ISSN 0925-2312, https://doi.org/10.1016/j.neucom.2024.127427.

[11] Iqbal, Zeeshan & Khan, Salim & Mehmood, Amjad & Lloret, Jaime & Alrajeh, Nabil. (2016). Adaptive Cross-Layer Multipath Routing Protocol for Mobile Ad Hoc Networks. Journal of Sensors. 2016. 1-18. 10.1155/2016/5486437.

[12] Kaiyang Guo, Yiliang Han, Riming Wu, Kai Liu, "CD-ABSE: Attribute-Based Searchable Encryption Scheme Supporting Cross-Domain Sharing on Blockchain", Wireless Communications and Mobile Computing, vol. 2022, Article ID 6719302, 15 pages, 2022. https://doi.org/10.1155/2022/6719302

[13] Li, Chao & Li, Fan & Yin, Lihua & Luo, Tianjie & Wang, Bin. (2021). A Blockchain-Based IoT Cross-Domain Delegation Access Control Method. Security and Communication Networks. 2021. 1-11. 10.1155/2021/3091104.

[14] Gholamreza Ramezan, Cyril Leung, "A Blockchain-Based Contractual Routing Protocol for the Internet of Things Using Smart Contracts", Wireless Communications and Mobile Computing, vol. 2018, Article ID 4029591, 14 pages, 2018. https://doi.org/10.1155/2018/4029591

[15] Mehbodniya, Abolfazl & Webber, Julian & Rani, Rashmi & Ahmad, Sayed & Wattar, Ihab & Ali, Liaqat & Nuagah, Stephen. (2022). Energy-Aware Routing Protocol with Fuzzy Logic in Industrial Internet of Things with Blockchain Technology. Wireless Communications and Mobile Computing. 2022. 1-15. 10.1155/2022/7665931.

[16] Yaohua Chen, Waixi Liu, "MAC Layer Energy Consumption and Routing Protocol Optimization Algorithm for Mobile Ad Hoc Networks", Complexity, vol. 2021, Article ID 6687189, 12 pages, 2021. https://doi.org/10.1155/2021/6687189

[17] Sheng Peng, Zhiming Cai, Wenjian Liu, Wennan Wang, Guang Li, Yutin Sun, Linkai Zhu, "Blockchain Data Secure Transmission Method Based on Homomorphic Encryption", Computational Intelligence and Neuroscience, vol. 2022, Article ID 3406228, 9 pages, 2022. https://doi.org/10.1155/2022/3406228

[18] Haipeng Li, Zhen Xu, "Routing Protocol in VANETs Equipped with Directional Antennas: Topology-Based Neighbor Discovery and Routing Analysis", Wireless Communications and Mobile Computing, vol. 2018, Article ID 7635143, 13 pages, 2018. https://doi.org/10.1155/2018/7635143

[19] An, Qi & Zhang, Yanhui & Guo, Chong & Liu, Ximing & Huang, Junjia & Zhang, Wenzhan & Zhang, Shijun & Zhan, Chao & Cai, Yuxiang. (2022). Anonymous Traceability Protocol Based on Group Signature for Blockchain. Security and Communication Networks. 2022. 1-10. 10.1155/2022/4559119.

[20] Thakur, Shashidhar & Chao, Kai-Yuan & Wong, D.F.. (1998). Minimum Crosstalk Vertical Layer Assignment for Three-Layer

VHV Channel Routing. VLSI Design. 7. 10.1155/1998/34910.

[21] Kannan Govindan, Preeti Jain, Rajesh Kr. Singh, Ruchi Mishra, Blockchain technology as a strategic weapon to bring procurement 4.0 truly alive: Literature review and future research agenda, Transportation Research Part E: Logistics and Transportation Review, Volume 181, 2024, 103352, ISSN 1366-5545, https://doi.org/10.1016/j.tre.2023.103352.

[22] Sotirios Messinis, Nikos Temenos, Nicholas E. Protonotarios, Ioannis Rallis, Dimitrios Kalogeras, Nikolaos Doulamis, Enhancing Internet of Medical Things security with artificial intelligence: A comprehensive review, Computers in Biology and Medicine, Volume 170, 2024, 108036, ISSN 0010-4825, https://doi.org/10.1016/j.compbiomed.2024.108036.

[23] Hai Ziwei, Zhang Dongni, Zhang Man, Du Yixin, Zheng Shuanghui, Yang Chao, Cai Chunfeng, The applications of internet of things in smart healthcare sectors: a bibliometric and deep study, Heliyon, Volume 10, Issue 3, 2024, e25392, ISSN 2405-8440, https://doi.org/10.1016/j.heliyon.2024.e25392.

[24] Fatima Alwahedi, Alyazia Aldhaheri, Mohamed Amine Ferrag, Ammar Battah, Norbert Tihanyi, Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models, Internet of Things and Cyber-Physical Systems, Volume 4, 2024, Pages 167-185, ISSN 2667-3452, https://doi.org/10.1016/j.iotcps.2023.12.003.

[25] Javier Pastor-Galindo, Félix Gómez Mármol, Gregorio Martínez Pérez, On the gathering of Tor onion addresses, Future Generation Computer Systems, Volume 145, 2023, Pages 12-26, ISSN 0167-739X, https://doi.org/10.1016/j.future.2023.02.024.

[26] Rathnakar Achary, Chetan J Shelke, Kavin Marx, Aishwarya Rajesh, Security Implementation on IoT using CoAP and Elliptical Curve Cryptography, Procedia Computer Science, Volume 230, 2023, Pages 493-502, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2023.12.105.

[27] Andrew J, Deva Priya Isravel, K. Martin Sagayam, Bharat Bhushan, Yuichi Sei, Jennifer Eunice, Blockchain for healthcare systems: Architecture, security challenges, trends and future directions, Journal of Network and Computer Applications, Volume 215,2023,103633,ISSN 1084-8045,https://doi.org/10.1016/j.jnca.2023.103633.

[28] Kebira Azbeg, Ouail Ouchetto, Said Jai Andaloussi, BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security, Egyptian Informatics Journal, Volume 23, Issue 2,2022,Pages 329-343,ISSN 1110-8665,https://doi.org/10.1016/j.eij.2022.02.004.

[29] Vika Crossland, Connor Dellwo, Golam Bashar, Gaby G. Dagher, Janus: Toward preventing counterfeits in supply chains utilizing a multi-quorum blockchain, Blockchain: Research and Applications, sVolume 4, Issue 4,2023,100157,ISSN 2096-7209, https://doi.org/10.1016/j.bcra.2023.100157.

[30] Olga Siedlecka-Lamch, Secure Medical Data Storage with Blockchain Technology, Procedia Computer Science, Volume 225,2023Pages 961-968,ISSN 1877-0509, https://doi.org/10.1016/j.procs.2023.10.083

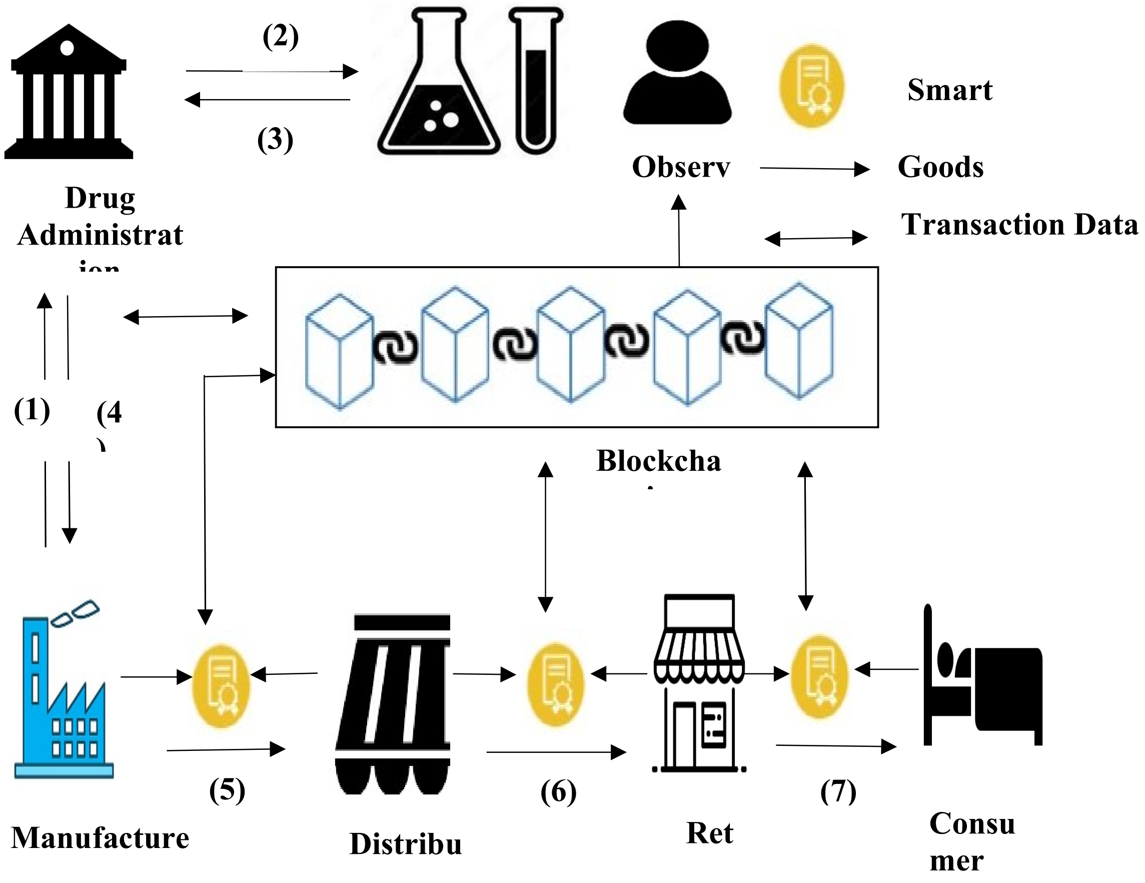


Figure 1: Traditional Healthcare Supply Chain Includes Partners

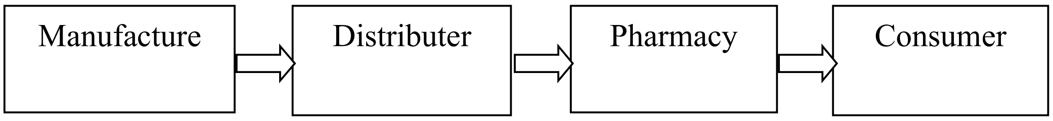


Figure 2: Blockchain-Enabled Pharmaceutical Supply Chain Process

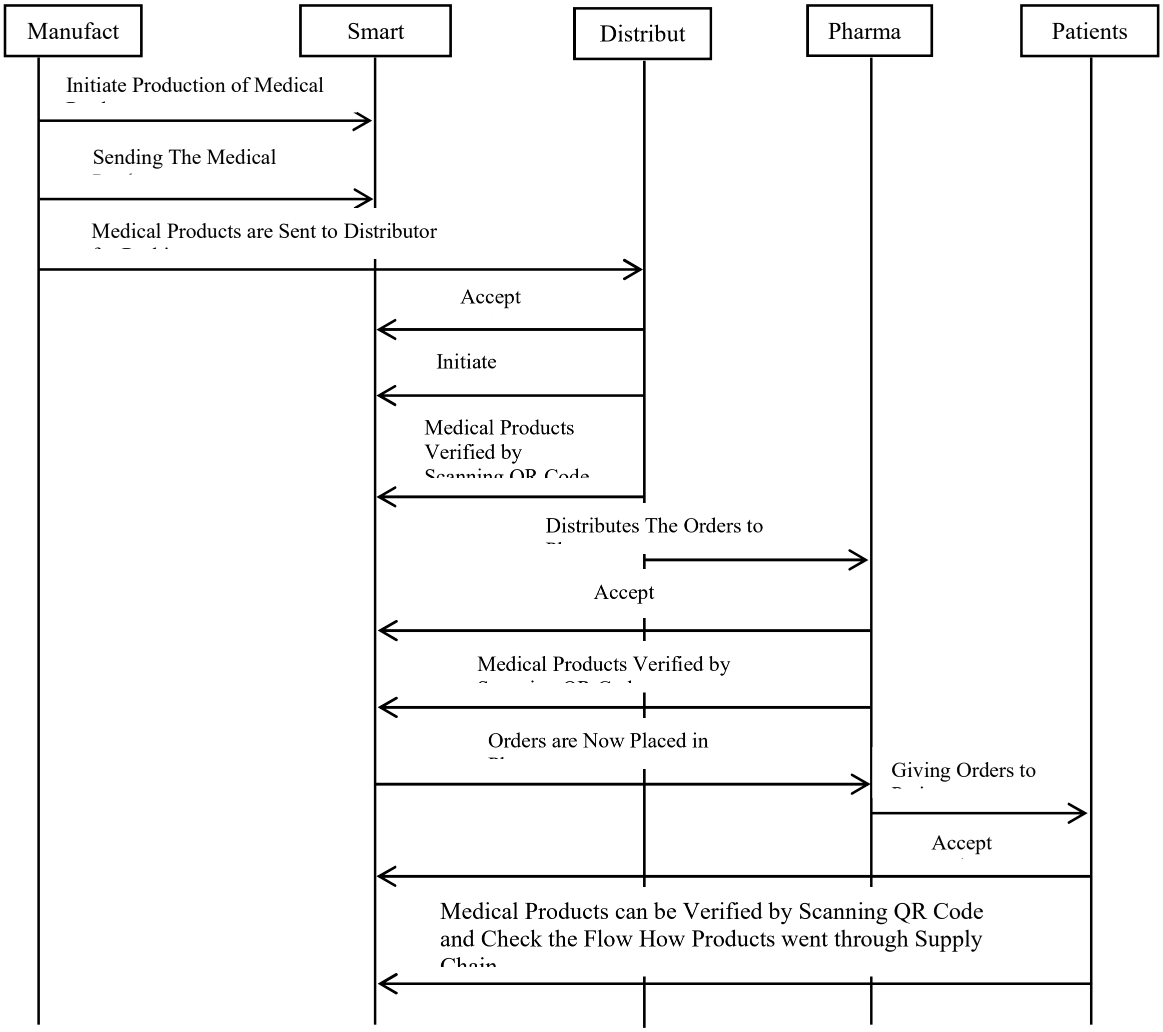
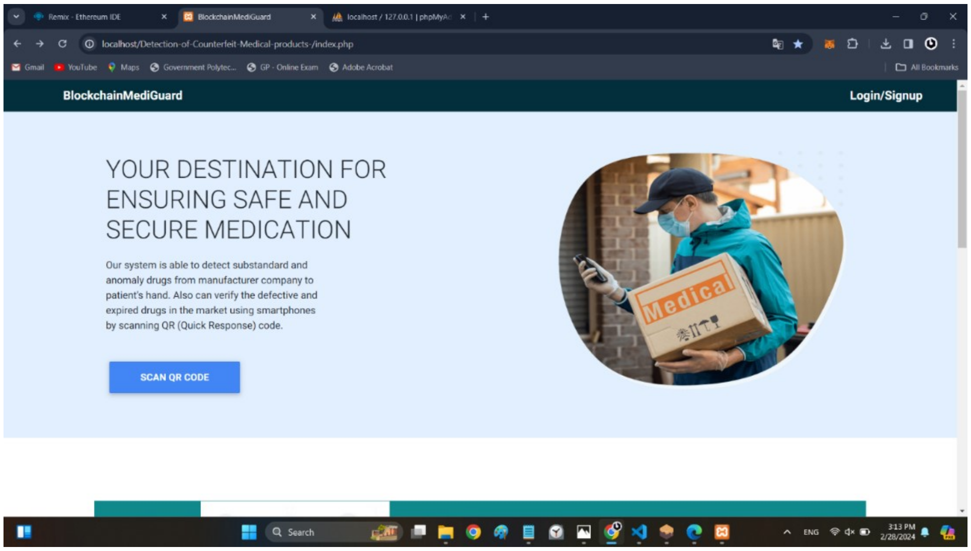

Manufact
Smart
Distribut
Pharma
Patients
Initiate Production of Medical
Sending The Medical
Medical Products are Sent to Distributor
Accept
Initiate
Medical Products Verified by Scanning QR Code
Distributes The Orders to
Accept
Medical Products Verified by
Orders are Now Placed in
Giving Orders to
Accept
Medical Products can be Verified by Scanning QR Code and Check the Flow How Products went through Supply Chain

Figure 3: Proposed Sequence Diagram



YOUR DESTINATION FOR ENSURING SAFE AND SECURE MEDICATION

Our system is able to detect substandard and anomaly drugs from manufacturer company to patient's hand. Also can verify the defective and expired drugs in the market using smartphones by scanning QR (Quick Response) code.

SCAN QR CODE

Figure 4: Dashboard of Medical Counterfeit

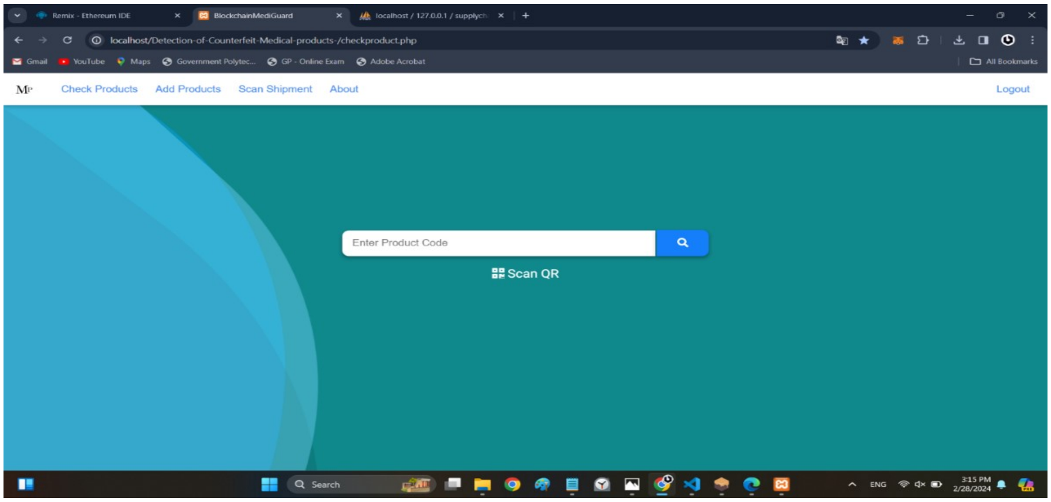
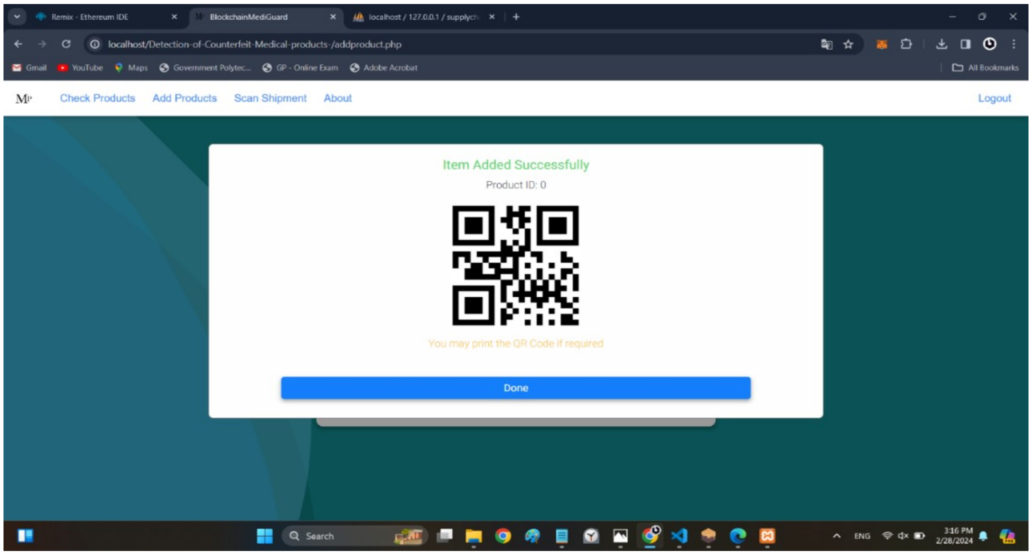


Figure 5: Product checking on platform



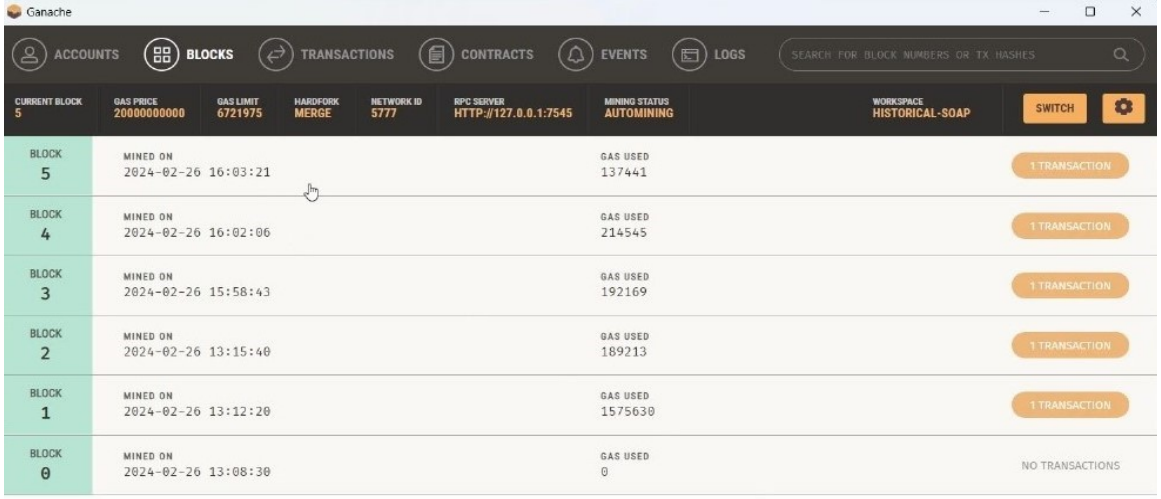
Item Added Successfully

Product ID: 0

You may print the QR Code if required

Done

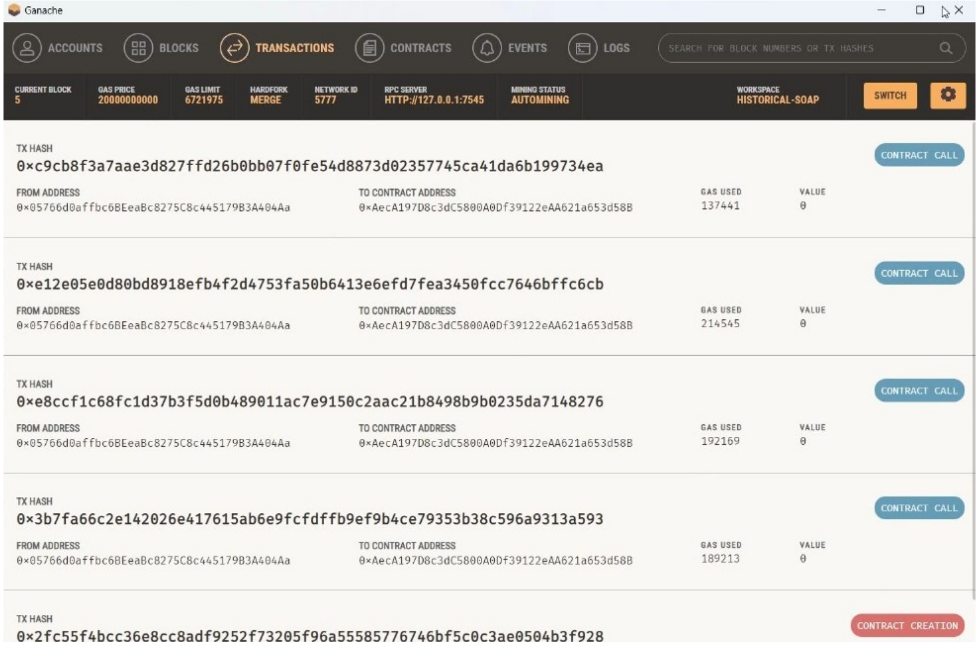
Figure 6: QR generated by manufacturer



CURRENT BLOCK 5 | GAS PRICE 20000000000 | GAS LIMIT 6721975 | HARDFORK MERGE | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:7545 | MINING STATUS AUTOMINING | WORKSPACE HISTORICAL-SOAP

BLOCK	MINED ON	GAS USED	
5	2024-02-26 16:03:21	137441	1 TRANSACTION
4	2024-02-26 16:02:06	214545	1 TRANSACTION
3	2024-02-26 15:58:43	192169	1 TRANSACTION
2	2024-02-26 13:15:40	189213	1 TRANSACTION
1	2024-02-26 13:12:20	1575630	1 TRANSACTION
0	2024-02-26 13:08:30	0	NO TRANSACTIONS

Figure 7: Ganache blocks simulation interface



CURRENT BLOCK 5 | GAS PRICE 20000000000 | GAS LIMIT 6721975 | HARDFORK MERGE | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:7545 | MINING STATUS AUTOMINING | WORKSPACE HISTORICAL-SOAP

TX HASH
0×c9cb8f3a7aae3d827ffd26b0bb07f0fe54d8873d02357745ca41da6b199734ea
CONTRACT CALL
FROM ADDRESS 0×05766d0affbc6BEeaBc8275C8c445179B3A404Aa
TO CONTRACT ADDRESS 0×AecA197D8c3dC5800A0Df39122eAA621a653d58B
GAS USED 137441
VALUE 0

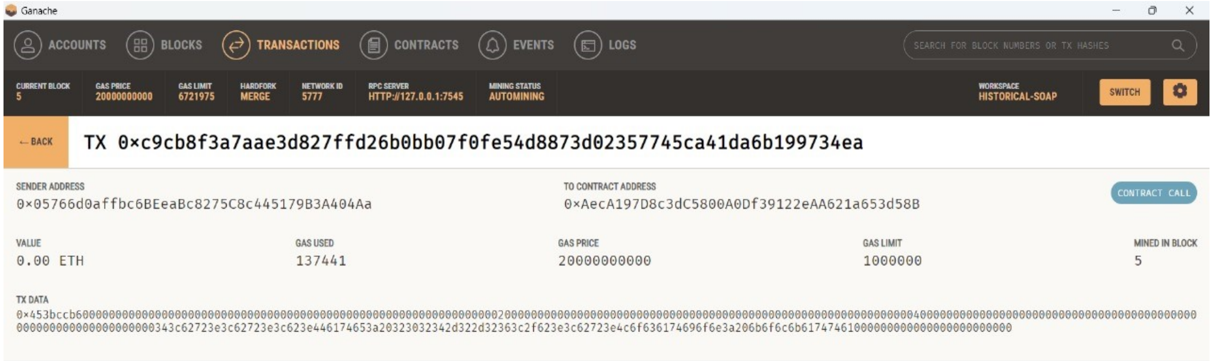
TX HASH
0×e12e05e0d80bd8918efb4f2d4753fa50b6413e6efd7fea3450fcc7646bffc6cb
CONTRACT CALL
FROM ADDRESS 0×05766d0affbc6BEeaBc8275C8c445179B3A404Aa
TO CONTRACT ADDRESS 0×AecA197D8c3dC5800A0Df39122eAA621a653d58B
GAS USED 214545
VALUE 0

TX HASH
0×e8ccf1c68fc1d37b3f5d0b489011ac7e9150c2aac21b8498b9b0235da7148276
CONTRACT CALL
FROM ADDRESS 0×05766d0affbc6BEeaBc8275C8c445179B3A404Aa
TO CONTRACT ADDRESS 0×AecA197D8c3dC5800A0Df39122eAA621a653d58B
GAS USED 192169
VALUE 0

TX HASH
0×3b7fa66c2e142026e417615ab6e9fcfdffb9ef9b4ce79353b38c596a9313a593
CONTRACT CALL
FROM ADDRESS 0×05766d0affbc6BEeaBc8275C8c445179B3A404Aa
TO CONTRACT ADDRESS 0×AecA197D8c3dC5800A0Df39122eAA621a653d58B
GAS USED 189213
VALUE 0

TX HASH
0×2fc55f4bcc36e8cc8adf9252f73205f96a55585776746bf5c0c3ae0504b3f928
CONTRACT CREATION

Figure 8: Ganache transaction on the local Ethereum



CURRENT BLOCK 5 | GAS PRICE 20000000000 | GAS LIMIT 6721975 | HARDFORK MERGE | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:7545 | MINING STATUS AUTOMINING | WORKSPACE HISTORICAL-SOAP

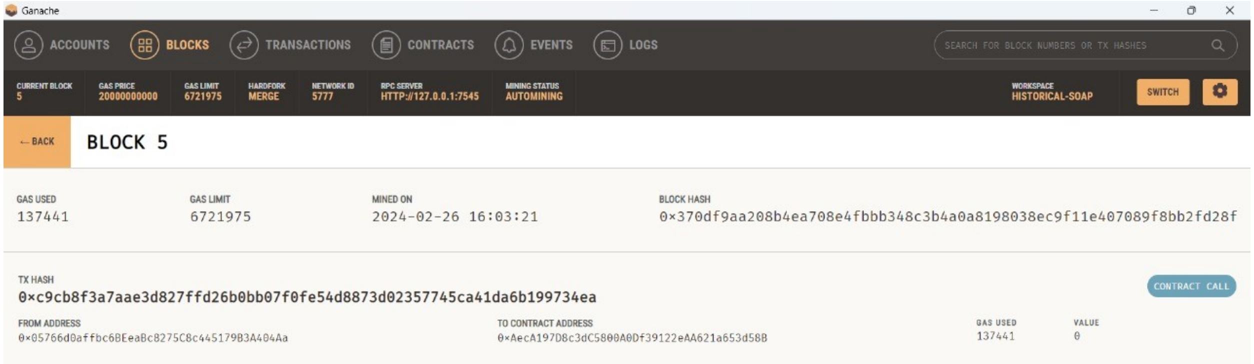
TX 0×c9cb8f3a7aae3d827ffd26b0bb07f0fe54d8873d02357745ca41da6b199734ea

SENDER ADDRESS 0×05766d0affbc6BEeaBc8275C8c445179B3A404Aa
TO CONTRACT ADDRESS 0×AecA197D8c3dC5800A0Df39122eAA621a653d58B
CONTRACT CALL

VALUE 0.00 ETH
GAS USED 137441
GAS PRICE 20000000000
GAS LIMIT 1000000
MINED IN BLOCK 5

TX DATA
```
0×453bccb600000000000000000000000000000000000000000000000000000000000000200000000000000000000000000000000000000000000000000000000000000040000000000000000000000000000000000000000000
00000000000000000000343c62723e3c62723e3c623e446174653a20323032342d322d32363c2f623e3c62723e4c6f636174696f6e3a206b6f6c6b61747461000000000000000000000000
```

Figure 9: Keccak Hashing for Transaction IDs in Blockchain for Medication Transactions



CURRENT BLOCK 5 | GAS PRICE 20000000000 | GAS LIMIT 6721975 | HARDFORK MERGE | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:7545 | MINING STATUS AUTOMINING | WORKSPACE HISTORICAL-SOAP

BLOCK 5

GAS USED 137441
GAS LIMIT 6721975
MINED ON 2024-02-26 16:03:21
BLOCK HASH 0×370df9aa208b4ea708e4fbbb348c3b4a0a8198038ec9f11e407089f8bb2fd28f

TX HASH 0×c9cb8f3a7aae3d827ffd26b0bb07f0fe54d8873d02357745ca41da6b199734ea
FROM ADDRESS 0×05766d0affbc6BEeaBc8275C8c445179B3A404Aa
TO CONTRACT ADDRESS 0×AecA197D8c3dC5800A0Df39122eAA621a653d58B
GAS USED 137441
VALUE 0

Figure 10: Details of Block in Local Ethereum Blockchain Environment

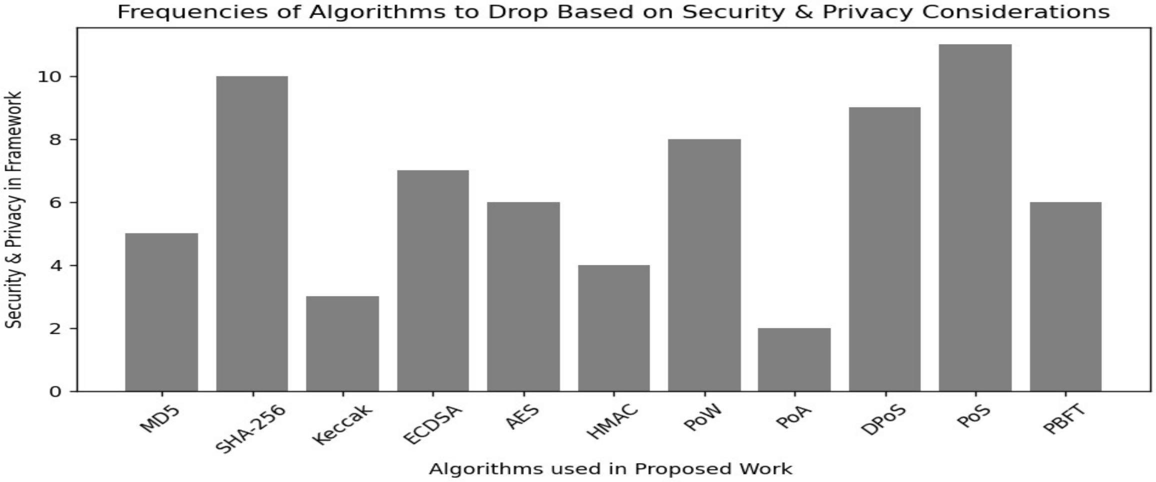


Figure 11: Frequencies of Algorithms to Drop Based on Security and Privacy Concerns

Table 1: Comparative Analysis of Previous Research and Our Approach.

Aspect	**Previous Approach**	**Our Approach**	**Algorithmic Evaluation in Blockchain Studies**
Technologies Used	✕	✓	Both studies leverage blockchain technology, but Our Approach incorporates additional tools like Remix IDE, Ganache, and MetaMask for blockchain development.
Focus Areas	✓	✓	Both approaches address specific challenges, but Our Approach focuses on combating counterfeit medical items in the supply chain.
Security Measures	✓	✓	Both approaches implement various security measures, but Our Approach includes a wider range of encryption algorithms and tools.
Specific Challenges Addressed	✓	✓	Both approaches address specific challenges, but Our Approach focuses solely on counterfeit medical items in the supply chain.
Entity Roles Defined	✓	✓	Both studies define distinct entity roles within the supply chain, ensuring transparency and accountability.
Data Storage	✕	✓	Our Approach explicitly mentions the use of XAMPP's MySQL database for secure data storage.
Verification Mechanism	✕	✓	Our Approach implements a user-friendly verification mechanism through QR code scanning and blockchain querying.
Privacy and Anonymity Measures	✕	✓	Our Approach employs Onion routing and various encryption techniques to ensure privacy and anonymity.
Impact on Businesses	✓	✓	Both studies aim to improve technology in their respective domains, with Our Approach focusing specifically on enhancing the medical supply chain.