Cyber Security and Applications 3 (2025) 100103

Contents lists available at ScienceDirect

Cyber Security and Applications

journal homepage: http://www.keaipublishing.com/en/journals/cyber-security-and-applications/

Secure and efficient drug supply chain management system: Leveraging polymorphic encryption, blockchain, and cloud storage integration

Muammar Shahrear Famous [a,*], Samia Sayed [a], Rashed Mazumder [a], Risala T. Khan [a], M. Shamim Kaiser [a], Mohammad Shahadat Hossain [b], Karl Andersson [c], Rahamatullah Khondoker [d]

[a] IIT, Jahangirnagar University, Savar, Dhaka, 1342, Bangladesh
[b] CSE, Chittagong University, Chittagong, 4331, Chittagong, Bangladesh
[c] CSESE, Luleå University of Technology, SE-97187, Skellefteå, Sweden
[d] THM University of Applied Sciences, Wilhelm-Leuschner-Str, Friedberg, 13 D - 61169, Germany

ARTICLE INFO

Keywords:
Polymorphic encryption
Blockchain
Cloud integration
SCMapp
SCR

ABSTRACT

The counterfeit medication infiltration within global supply chains poses a major public health threat. To address this, a collaborative effort among governments, regulators, and pharmaceutical companies is essential to secure the global/local supply chain. This paper proposes a novel approach that leverages blockchain technology, polymorphic encryption, and cloud storage to tackle security risks and privacy concerns in medication supply chains. The framework integrates a drug supply chain decentralized application (also called SCMapp) within the Ethereum blockchain, enabling functionalities like secure supplier onboarding, encrypted data management, cloud storage integration, and efficient data retrieval. This approach aims to revolutionize drug supply chain management by enhancing security, transparency, and overall efficiency, ensuring adherence to global health regulations. A safe and effective method for managing drug supply chains is provided by the suggested Drug Supply Chain Management System. The proposed model outperformed existing solutions in terms of security, efficiency, and traceability. The combination of encryption, blockchain, and cloud storage provided a comprehensive approach to address the challenges of drug supply chain management. The comparison analysis highlighted the unique advantages of the proposed model over other methods.

1. Introduction

The pharmaceutical industry is facing a critical challenge with the proliferation of counterfeit and substandard drugs in the global market. This issue poses significant risks to consumer safety, public health, and the integrity of the pharmaceutical supply chain. In 2022, pharmaceutical crime incidents surged to alarming levels, totaling 6,615 cases—a ten percent increase from the previous year. These incidents, spanning commercial and non-commercial seizures, involved a staggering variety of medicines, highlighting the complexity and impact of the problem across 141 countries worldwide [1,2]. With arrests related to pharmaceutical crime rising by 42 percent, it is evident that this is a pressing global crisis that demands immediate attention and concerted efforts to address effectively [3].

Fig. 1 illustrates the incidents of counterfeit crimes across different regions, providing insight into the global prevalence of pharmaceutical counterfeiting [4]. Existing research in the field of pharmaceutical supply chain management has identified several limitations that hinder the effectiveness of current systems. These include scalability issues, inadequate traceability measures leading to a high risk of data tampering, poor system efficiency and responsiveness, and a lack of interoperability [5]. These drawbacks highlight the urgent need for innovative solutions to enhance the traceability and security of pharmaceutical supply chains [6,7].

One promising approach is the integration of Blockchain, Cloud Storage and Polymorphic Encryption which offers transparency, immutability, and decentralization. By leveraging these technologies, a robust framework can be established to prevent the infiltration of counterfeit drugs and ensure patient safety on a global scale [8,9].

Peer review under the responsibility of KeAi Communications Co., Ltd.
* Corresponding author.
E-mail addresses: shahrear.stu2017@juniv.edu (M.S. Famous), samiaju47@gmail.com (S. Sayed), rmiit@juniv.edu (R. Mazumder), risala@juniv.edu (R.T. Khan), mskaiser@juniv.edu (M.S. Kaiser), hossain_ms@cu.ac.bd (M.S. Hossain), karl.andersson@ltu.se (K. Andersson), rahamatullah.khondoker@mnd.thm.de (R. Khondoker).

https://doi.org/10.1016/j.csa.2025.100103
Received 12 January 2025; Received in revised form 14 May 2025; Accepted 2 June 2025
Available online 6 June 2025

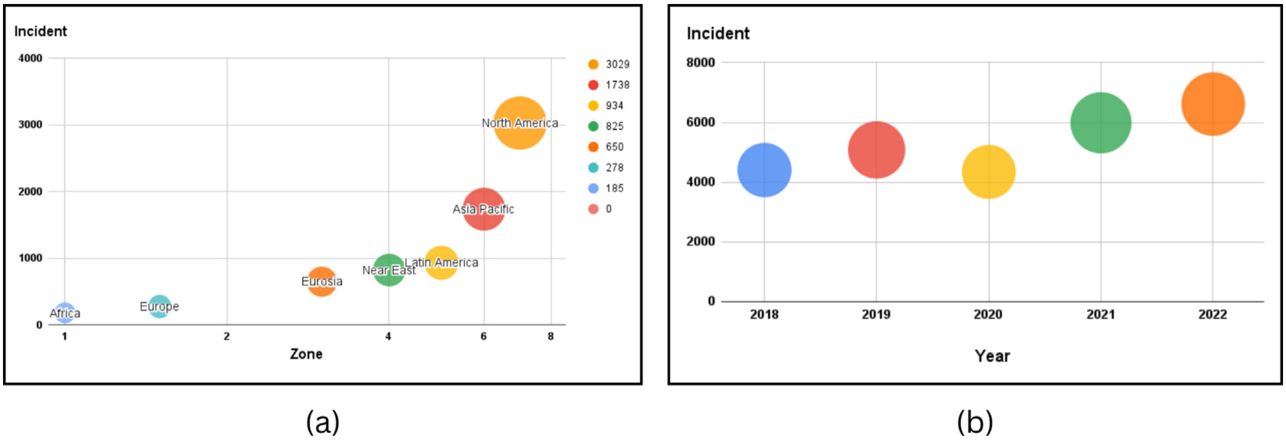

Fig. 1. A detailed analysis of counterfeit crimes, showing the global distribution and increasing incidences of pharmaceutical counterfeiting over time, as well as insights into regional patterns and changes in occurrences over time. Source: https://www.psi-inc.org.

This research significantly contributes to the drug supply chain management sector by introducing a framework aimed at enhancing data security and privacy. Our key contributions include:

- A decentralized consensus mechanism has been proposed to improve the transparency and integrity of supply chain transactions, establishing trust amongst stakeholders, and reduce the probability of unethical activities.
- We enhanced supply chain security by combining blockchain technology with cryptographic techniques that include polymorphic encryption.
- We developed a comprehensive design for smart contract deployment, focusing on its pivotal role in securely managing medicine and supplier details within the supply chain management.

The rest of the paper is structured as follows. Section 2 discusses the existing works. Section 3 introduces the proposed system framework, Section 4 discusses the result analysis of the framework and finally a conclusion is drawn in Section 5.

2. Related work

This section explores into existing research in three pivotal domains: Blockchain application in Drug Supply Chain Management, approaches integrating Cloud Storage, and solutions leveraging Polymorphic Encryption.

Abbas et al. [10] introduced a blockchain-based drug supply chain management and recommendation (DSCMR) system based on machine learning and blockchain to improve traceability and reduce counterfeit drugs in the pharmaceutical supply chain (3). While their dual-module approach—using Hyperledger Fabric for drug tracking and machine learning models (N-gram, LightGBM) for drug recommendation —shows promising results, the system has some limitations. The authors acknowledge that their current implementation is simulated and limited in network size, which may not reflect real-world performance. Additionally, the machine learning models rely on public review data, which may affect the accuracy and generalizability of drug recommendations. The authors suggest future work should involve deploying the system in real-time pharmaceutical environments and improving the machine learning models for better prediction accuracy and reliability. Dana et al. [11] focused on providing governance within the pharmaceutical supply chain using blockchain and machine learning. This approach seeks to ensure transparency and accountability, which are crucial for preventing fraud and maintaining compliance. However, they did not develop a decentralized application (dApp), raising concerns about the practical implementation of their system. The absence of a dApp may limit user interaction and reduce the system's overall functionality.

Vincent et al. [12] aimed to enhance supply chain security with a combination of blockchain and artificial intelligence. The study suggests that integrating these technologies can provide stronger protection against tampering and fraud. Their study lacks a clear implementation methodology, which leaves uncertainty about how their proposed solutions can be practically applied. This gap may hinder the adoption of their approach in real-world scenarios. Ranjana et al. [13] proposed a public blockchain system to prevent drug counterfeiting using AI, QR codes, RFID, and NFC. The system aims to improve the verification and traceability of pharmaceutical products. But, their methodology lacks experimental validation, which raises concerns about its effectiveness in real-world applications. Without proper validation, the system's reliability remains uncertain.

Ahmadi et al. [14] explored an IoT-based blockchain framework to combat counterfeit drugs by improving traceability, security, and transparency in the pharmaceutical supply chain. They explained technical components like hashing, encryption, and RFID integration. However, the paper lacks experimental validation, real-world implementation, and performance metrics. It also does not address regulatory compliance or interoperability with existing healthcare systems. Pilot studies, integration with legal frameworks, and an analysis of system scalability and cost-effectiveness could have provided a better understanding of the process. Singh et al. [15] sought to control drugs' authenticity using a private blockchain and IoT. The study highlights the potential of combining these technologies to enhance security in the supply chain. Yet, the work has limited fault tolerance, which may affect the system's robustness and reliability. This limitation could lead to vulnerabilities in the supply chain if the system fails under certain conditions. Xiaohong et al. [16] aimed to enhance supply chain resilience through blockchain and IoT. Their approach focuses on improving the adaptability and reliability of the supply chain in response to disruptions. Although, they didn't provide details on the supply chain operations reference (SCOR) implementation process, leaving room for practical refinement. Without clear guidance on implementation, the proposed system may be difficult to apply in real-world scenarios. The life cycle of a blockchain system is shown in Fig. 2. This covered the creation of a blockchain, transaction processing, validation, and finalization.

Altigani et al. [17] suggested the use of polymorphic encryption to protect different types of data. This method is designed to provide strong protection against unauthorized access. However, they highlight a significant drawback in its high implementation cost, which could limit its adoption. The cost factor may be a barrier for organizations with limited resources. Booher et al. [18] suggest polymorphic encryption as a shield against frequency analysis vulnerabilities in block ciphers. Their approach aims to enhance the security of encrypted data. Nevertheless,

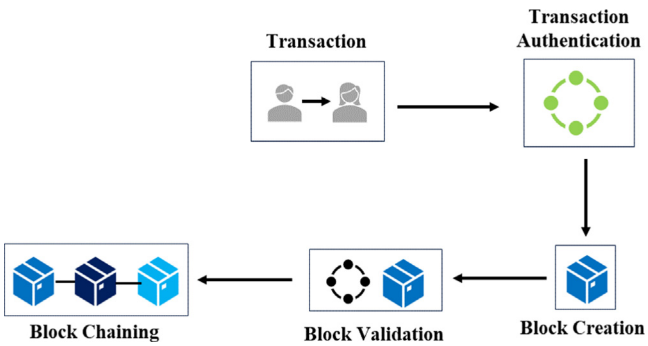

Fig. 2. Lifecycle of a Blockchain System, encompassing creation, transaction processing, validation, and finalization stages with detailed processes [33].

its widespread use is impeded by hardware limitations, which could restrict its applicability. These limitations may prevent the system from being implemented on a larger scale.

Meng et al. [19] tackle security among sensors with identity-based cryptography. This approach is intended to secure communication between sensors in the supply chain. They highlighted computational overhead as a concern, which could impact the system's efficiency. The added processing requirements may slow down operations and increase costs. Shim et al. [20] went for anonymity through lattice-based methods, favoring homomorphic encryption for its efficacy. These methods aim to protect user privacy while maintaining data security. However, the complexity of these techniques may pose challenges for implementation. The need for specialized knowledge could limit the system's adoption. Simion et al. [21] explore lockable obfuscation and RMERS-based public key encryption. They suggest various other public key encryption schemes for consideration, each with its own strengths and weaknesses. These methods offer different levels of security, but their practical application may require further testing. The diversity of options may complicate the decision-making process for choosing the best encryption method. Xie et al. [22] inquire post-quantum cryptography for comprehensive instrument security. Their study focuses on preparing for future threats posed by quantum computing. Yet, real-world implementation remains unfulfilled, which means the proposed solutions have not yet been tested in practice. This gap may delay the adoption of these advanced security measures.

KIM et al. [23] and Merrad et al. [24] look into isogeny-based digital signatures and game theory with random selection, respectively. Both studies highlight the complexity of their implementation processes, which could pose challenges for practical application. The advanced nature of these methods may require specialized knowledge and resources. The complexity may also increase the cost and time needed for deployment. Dashtizadeh et al. [25] suggested a way ti detect counterfeit drugs but didn't develop the proposed solution. Their study identifies the need for secure verification methods in the pharmaceutical supply chain. However, the lack of a dApp limits the system's functionality and user interaction. This omission may reduce the effectiveness of their proposed solution.

Ahmed et al. [26] provided vaccines authentically but lacked privacy measures. Their approach focuses on ensuring the authenticity of vaccines in the supply chain. But, the absence of privacy protection raises concerns about the security of sensitive data. This gap could lead to data breaches and undermine trust in the system. Musamih et al. [27] controlled drug authenticity but had immutability limitations. Their system aims to prevent tampering and fraud in the pharmaceutical supply chain. However, the limitations in immutability could allow unauthorized changes to the data, compromising the system's integrity. This issue may reduce confidence in the accuracy and reliability of the information.

Mohit et al. [28] traced drugs but had transaction rate issues. Their approach is designed to enhance the traceability of pharmaceutical products throughout the supply chain. The system's transaction rate issues could slow down operations, leading to delays and inefficiencies. These problems may hinder the system's ability to handle high volumes of transactions. Saindane et al. [29] traced drugs without smart contracts. Their study emphasizes the importance of tracking pharmaceutical products to ensure safety and compliance. However, the lack of smart contracts may reduce automation and increase the risk of human error. This limitation could affect the accuracy and reliability of the supply chain. Marbouh et al. [30] traced medicine but lacked a dApp. Their system aims to improve the traceability of medical products in the supply chain. The absence of a decentralise application limits the system's usability and interaction with users. This gap may reduce the effectiveness of their proposed solution.

Debe et al. [31] identified counterfeit drugs but didn't develop a dApp. Their study highlights the need for secure verification methods to combat counterfeiting in the pharmaceutical supply chain. However, the lack of a dApp reduces the system's functionality and ease of use. This limitation may hinder the adoption of their solution. Chang et al. [32] explored blockchain in the supply chain without addressing interoperability. Their study suggests that blockchain can enhance transparency and security in supply chain management. However, the lack of interoperability between different systems could limit the effectiveness of the solution. This gap may prevent seamless integration with other supply chain technologies.

Sahoo et al. [34] tackled tampering without smart contracts. Their approach aims to prevent unauthorized changes to data in the supply chain. However, the absence of smart contracts reduces automation and may increase the risk of errors. This limitation could affect the accuracy and reliability of the system. Jamil et al. [35] controlled authenticity but didn't deploy in a real setting. Their study emphasizes the importance of verifying the authenticity of pharmaceutical products in the supply chain. However, the lack of real-world deployment raises questions about the system's practicality and effectiveness. This gap may delay the adoption of their solution.

Pham et al. [36] traced drugs without optimized smart contracts. Their approach is designed to improve the traceability of pharmaceutical products in the supply chain. But, the lack of optimization in smart contracts may reduce the system's efficiency and performance. This issue could lead to delays and increased costs. Jayaraman et al. [37] tracked products but didn't mention dApp construction. Their study focuses on monitoring the movement of pharmaceutical products in the supply chain. Yet, the absence of a real life pplication raises concerns about the system's usability and interaction with users. This gap may limit the effectiveness of their proposed solution.

He et al. [38] pioneered a method combining encryption and data mining to strengthen cloud security. Their study aims to protect sensitive data in cloud-based supply chains. They address potential overhead costs, which could impact the system's performance and efficiency. However, the study highlights the importance of innovative strategies for practical implementation to overcome these challenges. Mani et al. [39] addressed counterfeit drugs with a private blockchain and cloud computing. Their approach focuses on securing the pharmaceutical supply chain to prevent the distribution of counterfeit products. But, their approach lacks comprehensive resource optimization, which may impact supply chain efficiency. This limitation could lead to increased costs and reduced performance in large-scale operations.

Xu et al. [40] propose a sanitizable signature scheme aimed at ensuring privacy protection in electronic medical data sharing. Their approach focuses on building a cryptographic solution that allows for privacy-preserving data sharing, specifically through a key-exposure-free chameleon hash technique. This method ensures that medical data remains confidential and can be shared securely across different entities. While the approach is promising in enhancing privacy, its application is primarily focused on cryptographic techniques without addressing the broader challenges in drug supply chain management, such as scalability and integration with existing systems. Rahaman et al. [41] introduce a framework based on Hyperledger Fabric technology to create a secure and sustainable food processing supply chain, emphasizing blockchain's role in ensuring data integrity, traceability, and security. While the framework is primarily focused on the food industry, its approach to secure data management is highly relevant to the pharmaceutical supply chain as well. However, the study faces limitations due to its private blockchain structure, which may hinder scalability when applied to more complex supply chains, such as those found in the pharmaceutical industry. Despite demonstrating improvements in transparency and accountability within food supply chains, the framework's scalability challenges and high implementation costs remain significant barriers. Including future research directions such as addressing scalability challenges, integrating emerging technologies like AI and IoT, and adapting the framework for larger, more complex supply chains would further strengthen the study and enhance its broader applicability.

Alqudhaibi et al. [42] examine the cybersecurity challenges in Industry 4.0, particularly within the manufacturing management sector. Their research assesses the various cybersecurity threats and proposes strategies to mitigate these risks. Although this study does not directly address drug supply chains, the emphasis on cybersecurity is highly relevant, as drug supply chains face similar vulnerabilities. A key limitation of this work is the lack of real-life application, which limits the practical impact of the proposed strategies in actual supply chain environments. Javaid et al. [43] provide a comprehensive review of cybersecurity practices and trends within the healthcare domain. The focus of their study is on ensuring cybersecurity within healthcare, which shares common challenges with the pharmaceutical supply chain. Their review highlights the critical need for robust cybersecurity measures to protect sensitive data. This study does not include real-life application, which limits its direct applicability to drug supply chains that require tested and deployable solutions.

Agrawal et al. [44] explore the adoption of blockchain technology to develop a secure healthcare solution. Their research is centered on creating a deployable, secure solution that leverages the benefits of public blockchain. While this approach has the potential to enhance security and transparency in healthcare data management, it also introduces privacy issues. These privacy concerns are particularly critical when considering the sensitive nature of drug supply chains, where patient and proprietary information must be carefully protected. Crossland et al. [45] propose a multi-quorum blockchain solution called Janus to prevent counterfeits in supply chains. The study emphasizes the importance of blockchain in maintaining the integrity of supply chains by preventing counterfeit products. The blockchain model used is private and lacks cloud storage, which limits its scalability and flexibility in larger, more complex supply chains, such as those in the pharmaceutical industry.

Javaid et al. [46] conduct a literature-based review on the applications of blockchain technology in Industry 4.0. The review highlights the potential benefits of blockchain in enhancing transparency and security in various industries. The study does not include real-life applications, which weakens the relevance of the findings to practical drug supply chain management. Cao et al. [47] introduce a blockchain-based multisignature approach for governance within the Australian beef supply chain. The study focuses on achieving transparent supply chain management, demonstrating the value of blockchain in food supply chains. However, the solution is limited to private blockchains and is specific to the Australian context, making it less applicable to global drug supply chains that require broader applicability and scalability.

Bottoni et al. [48] explore Blockchain-as-a-Service and Blockchain-as-a-Partner as options for optimizing supply chain management. The study discusses how blockchain can secure supply chains and improve efficiency. While the study offers insights into the potential applications of blockchain in supply chain management, it lacks detailed exploration of real-life applications. Which is a significant gap when considering the implementation of these technologies in drug supply chains. Vaghani et al. [49] provide a solution on the security and Quality of Service (QoS) issues in blockchain-enabled next-generation smart logistic networks. Their study emphasizes the importance of intelligent blockchain-based systems in managing supply chains. Similar to other studies, this work lacks real-life application examples, which limits its direct applicability to drug supply chains that require tested and deployable solutions.

Adam et al. [50] explore the benefits of adopting blockchain technology. The focus is on creating a sustainable and transparent system using public blockchain. However, the study does not dig into the details of real-life application, which is crucial for implementing such solutions in drug supply chains where legal and regulatory considerations are significant. Regueiro et al. [51] propose a blockchain-based refurbishment certification system aimed at enhancing the circular economy. The study emphasizes the role of blockchain in promoting sustainability. But, the application is focused on general circular economy principles and lacks depth concerning its applicability to the pharmaceutical industry, which has specific requirements related to drug lifecycle management and regulatory compliance.

Akshatha et al. [52] discuss a method for user-controlled data access using MQTT and blockchain sharding. The study aims to improve security and efficiency in data access. The approach introduces challenges related to data storage, which is a critical consideration in drug supply chains where secure and efficient data management is paramount. Chen et al. [53] explore security challenges and defense approaches for blockchain-based services from a full-stack architecture perspective. Their study provides insights into securing blockchain services but lacks real-life application examples, limiting its relevance to drug supply chains that require proven, practical solutions for managing security risks.

Allenbrand et al. [54] propose the use of smart contract-enabled consortium blockchains to control information distortion within supply chains. The study highlights the potential of blockchain to improve information accuracy. The absence of cryptographic mechanisms in their approach poses a significant limitation, as drug supply chains require robust cryptography to ensure the integrity and confidentiality of sensitive information. Sarfaraz et al. [55] conduct a simulation study on the implications of blockchain-coordinated information sharing within a supply chain. The study shows the potential of blockchain to enhance coordination and information sharing. As with several other studies, the lack of real-life application examples diminishes its direct applicability to drug supply chains, which require solutions that have been tested in real-world scenarios.

Cui et al. [56] focus on securing the vaccine circulation process using a consortium blockchain. Their study emphasizes the role of blockchain in ensuring the integrity and security of vaccine distribution. This approach is significant for maintaining the safety of vaccine supply chains, though the consortium nature of the blockchain might limit its scalability across different stakeholders in global drug supply chains. Omar et al. [57] explore the tracing of personal protective equipment (PPE) using a public blockchain. The study aims to enhance the transparency and accountability of PPE distribution. The use of public blockchain ensures broad accessibility and transparency. This is crucial for supply chains requiring public trust, such as those handling medical supplies during pandemics.

Mahdiraji et al. [58] aim to ensure proper drug traceability using the Pythagorean Fuzzy-Delphi method. Their approach provides a structured way to handle uncertainty in drug traceability. The study does not utilize blockchain or other modern digital technologies. This may limit its effectiveness in highly complex drug supply chains. Kumar et al. [59] focus on the proper supply chain management (SCM) of medical equipment using artificial intelligence. The study highlights how AI can optimize the management and distribution of medical equipment. Although the use of AI is promising, the study does not integrate blockchain or other technologies that could enhance traceability and security in the supply chain, which are critical for drug supply chains.

Table 1
Classification of Blockchain: This table categorizes different types of blockchain including public, private, hybrid, etc., based on their characteristics.

Public	Private	Hybrid	Consortium
Open to the public. Anyone can join, read, and write transactions.	Restricted access, typically for a specific organization or group.	Combination of public and private features, offering flexibility.	Shared by multiple organizations, each with certain control.
Bitcoin, Ethereum	Multichain, Hyperledger Fabric (single org)	Binance Chain, IBM Blockchain	Corda, Hyperledger Sawtooth, Quorum

Table 2
Overview of recent technological adoptions in supply chain management and their associated limitations. The table highlights challenges like scalability, implementation complexity, and lack of validation across various emerging technologies.

Reference	Based On	Limitations
[10]	Private Blockchain, ML	Scalability issues due to network size constraints.
[11]	Blockchain, ML	Lack of decentralized application (dApp) development.
[13]	Blockchain, AI, QR codes, RFID, NFC	Lack of experimental validation.
[14,64,65]	Blockchain, Holochain IoT	Issues with scalability and privacy in controlling drug authenticity.
[18]	Polymorphic encryption	High implementation cost and hardware limitations hindering widespread use of polymorphic encryption algorithms.
[21]	RMERS-based public key encryption	Various public key encryption schemes suggested for consideration, but concrete implementation models lacking.
[23,24]	Isogeny-based digital signatures	Complexity in the implementation processes of isogeny-based digital signatures and game theory with random selection.
[38]	Blockchain, Cloud Storage	Concerns about computational overhead in security among sensors.

Liu et al. [60] propose a sustainable supply chain management system by integrating AI, Big Data, Blockchain, and the Internet of Things (IoT). This comprehensive approach aims to enhance the sustainability and efficiency of supply chains. The study is highly relevant for modern drug supply chains that require a multifaceted approach to manage complex logistics, though the integration of these technologies poses challenges in implementation and coordination. Li et al. [61] address the proper traceability of medical equipment using blockchain technology. The study underscores the importance of blockchain in ensuring the accurate tracking of medical equipment. However, the lack of detail regarding the specific type of blockchain used and its scalability limits the study's applicability to large-scale drug supply chains.

Chithaluru et al. [62] focus on the traceability of drug supply using a combination of blockchain and IoT. The use of both technologies aims to enhance the precision and reliability of drug traceability. The public nature of the blockchain ensures transparency, which is vital for drug supply chains where trust and accountability are critical. Bistarelli et al. [63] propose an automated blockchain-based drug traceability system using a hybrid blockchain approach. This study aims to combine the strengths of both public and private blockchains to create a more robust and flexible system. The hybrid approach offers a balance between transparency and control, making it suitable for drug supply chains that require both public accountability and private management of sensitive data.

Koshiry et al. [66] explore the application of blockchain technology in the education system. Although the study is not directly related to drug supply chains, it highlights the versatility of blockchain to ensure transparency and accountability in various sectors. The insights gained from this study could be adapted to improve the traceability and management of information in drug supply chains. Kumar et al. [67] proposed a lightweight RFID authentication protocol for IIoT-enabled supply chains, combining edge computing and blockchain to enhance mutual authentication and data security. However, their approach may face challenges such as vulnerability to side-channel attacks on constrained devices and reliance on simulation-based evaluations, which may not fully reflect real-world deployment complexities such as synchronization delays or physical tampering of RFID tags.

Rupa et al. [68] developed a blockchain-based decentralized application (DApp) for drug supply chain management integrated with an AI-driven drug recommender system to improve transparency, traceability, and user interaction. Their system leverages Ethereum and the Sepolia testnet to optimize gas costs and scalability while ensuring secure, authorized data exchange across entities. The integration of a ResNet-based deep learning model achieved 92 percent accuracy in drug recognition. However, reliance on public blockchain raises concerns about scalability and privacy, and the recommended system may suffer from biases in training data and high computational requirements. Table 1 presents the classifications of blockchain, highlighting the key distinctions among them.

Table 2 provides an overview of technology adoption within supply chain management, including architectures and associated limitations.

3. Proposed methodology

Existing research on blockchain-based pharmaceutical supply chain management highlights several critical gaps that our proposed solution addresses. These include the need for real-world implementation to validate theoretical feasibility, discussions on scalability and consensus mechanisms, the absence of key components like dApps and smart contracts, and the importance of practical experiments and resource optimization. By addressing these gaps, our solution aims to enhance the safety, reliability, and efficiency of drug traceability and supply chain management in the pharmaceutical industry through blockchain integration.

3.1. Framework description

The framework involved integrating blockchain technology, polymorphic encryption and cloud storage into the supply chain management (SCM) model, developing smart contracts for traceability and security, establishing data sharing protocols, and creating a controlled testing environment.

3.1.1. Drug supply chain management system decentralized application (SCMapp)

The proposed Supply Chain Management Decentralized Application (SCMapp) architecture presents a robust, secure, and scalable framework for managing pharmaceutical supply chains by leveraging a synergy of blockchain technology, cloud storage, group signature-based identity verification, and polymorphic encryption. Fig. 3 illustrates the decentralized process of storing, accessing, and verifying data in supply

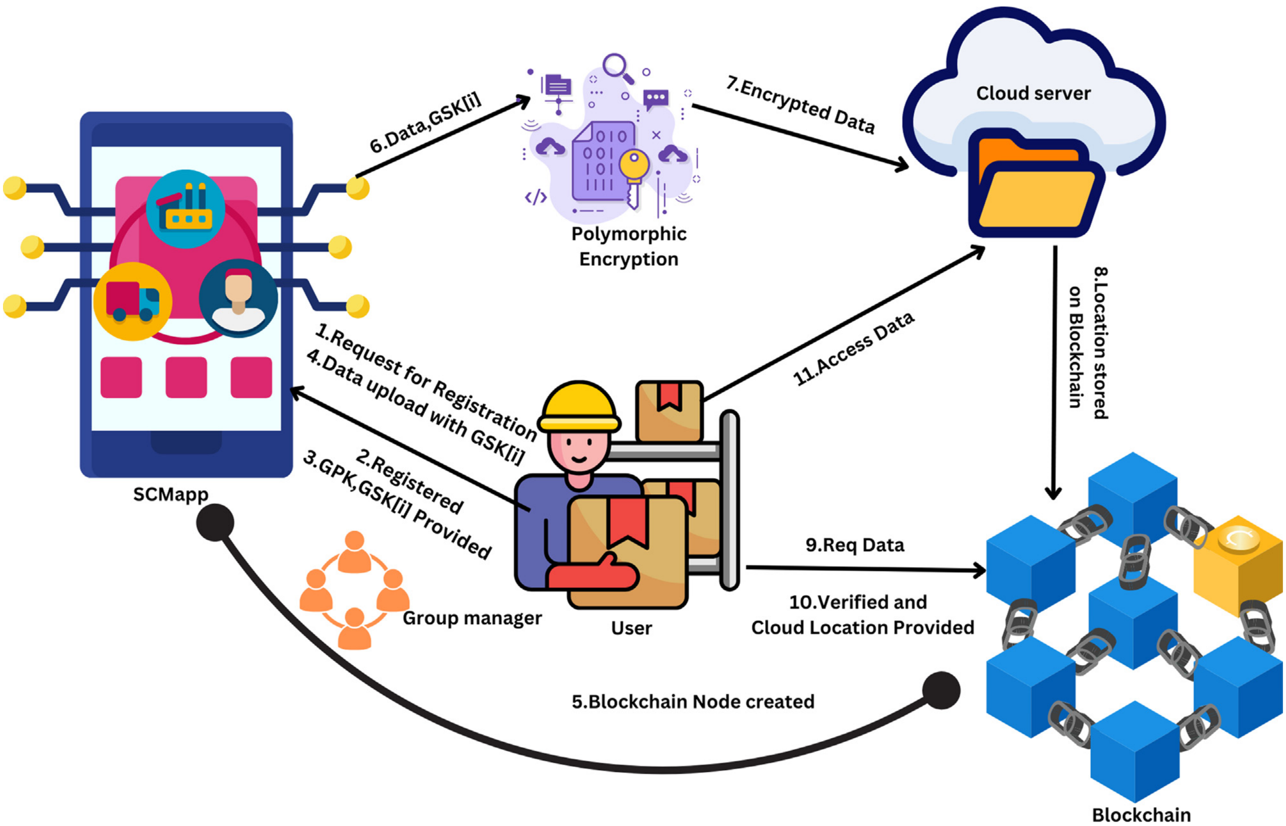

Fig. 3. A Blockchain-enabled Architecture for Drug Supply Chain Management Traceability: A Step-by-Step Process Flow Including User Registration, Data Encryption, Blockchain Node Creation, Verification, and Cloud Access Management.

chain management. A supplier, distributor, or manufacturer who is involved in the supply chain submits a registration request through the SCMapp to start the process.

A trusted authority identified as the Group Manager authenticates this request and, after successful validation, provides the registrant with a Group Public Key (GPK) and a distinct Group Secret Key (GSK[i]). After registering, the user creates relevant drug supply information, such as the source, batch numbers, shipping records, and regulatory certifications. Then, in order to improve data security and prevent potential cryptographic attacks, this data is encrypted using a polymorphic encryption process that dynamically changes encryption patterns. A third-party cloud server receives the encrypted data for off-chain storage, greatly lowering the blockchain's load and improving system scalability. By creating a lightweight blockchain node linked to the user, only the metadata or the location of the encrypted cloud data is kept on the blockchain to preserve data integrity and traceability. The user initiates a secure request through SCMapp when data retrieval is necessary. This request undergoes validation through the blockchain using group signature verification, ensuring that only legitimate and authorized participants can access the stored information. The corresponding cloud storage location of the encrypted data is given by the blockchain after a successful verification. In order to guarantee end-to-end security and data integrity, the user can then access the encrypted file from the cloud and use their GSK[i] to decrypt it. This secure and decentralized process improves the safety, transparency, and reliability of the drug supply chain by solving problems like fake medicines, unauthorized access, and poor tracking.

3.1.2. Supplier registration and authentication

Medicine suppliers must register with the SCM network to take part safely and securely in the decentralized supply chain system. This registration process is described in a systematic way in Algorithm 1.

Algorithm 1 Registration Process

1: **procedure** REG(S)
2: Let $Reg(S)$ denote the registration function for supplier S.
3: Supplier S initiates the registration process by providing necessary information.
4: The SCM system generates cryptographic keys and identifiers for the supplier.
5: Unique Identifier ID_S is assigned to supplier S.
6: Group Public Key: GPK is generated for secure communication within the supplier group.
7: Group Secret Key: $GSK[i]$ is assigned to supplier S for cryptographic operations.
8: **Mathematically:** $ID_S, GPK, GSK[i] = \text{Reg}(S)$.
9: **end procedure**

The process starts when a supplier S sends a registration request to the SCM system with their identification and business information. Such identification may include contact details, license documents, company information, and digital signatures. Upon receiving the registration request, the SCM system invokes the registration function Reg(S), which is responsible for generating a unique set of cryptographic credentials for the supplier. These include a Unique Identifier (ID_S), a Group Public Key (GPK), and a Group Secret Key ($GSK[i]$). The unique identifier ID_S serves as a permanent reference for the supplier within the SCM network, enabling traceability and accountability of all actions taken by the supplier. The Group Public Key (GPK) is a shared key accessible to all members within the supplier group and is used to establish secure and authenticated communication across the network. In contrast, the Group Secret Key ($GSK[i]$) is uniquely assigned to each registered supplier and is known only to that specific entity. This secret key enables the supplier to perform operations such as secure message exchange, while preserving their anonymity within the group through the use of group signature techniques. The system securely provides the generated keys to the supplier S after the registration process is finished. The Drug Supplier Management Blockchain is a tamper-proof ledger that securely stores these keys and IDs. This guarantees that the login credentials from registration may be used to validate all subsequent operations, such as data uploads and transaction tracking. By ensuring that only approved suppliers are allowed to join the supply chain, the registration procedure raises the decentralized SCM network's reliability and trustworthiness.

Algorithm 2 Data Encryption and Decryption

procedure GENKEY
  Dynamically generate a new encryption and decryption key pair ($KeyEn$, $KeyDec$) using `GenKey()`.
end procedure
procedure CHOOSEENCALG
  Randomly select an encryption algorithm $EncAlg$ from a predefined set {`XOR`, `AES`, `SHA`-based masking, etc.}.
end procedure
procedure ENCRYPT(Data)
  Call `GENKEY()` to generate fresh $KeyEn$ and $KeyDec$.
  Call `CHOOSEENCALG()` to randomly select an encryption algorithm $EncAlg$.
  if $EncAlg ==$ `XOR` **then**
    Generate a random number n.
    $Encrypted\_Data \leftarrow Data \oplus n$
  else if $EncAlg ==$ `AES` **then**
    $Encrypted\_Data \leftarrow AES\_Encrypt(Data, KeyEn)$
  else if $EncAlg ==$ `SHA`-based masking **then**
    $Encrypted\_Data \leftarrow Data \oplus SHA256(KeyEn)$
  end if
  return ($Encrypted\_Data, KeyDec, EncAlg, n$)
end procedure
procedure DECRYPT(Encrypted_Data, KeyDec, EncAlg, n)
  if $EncAlg ==$ `XOR` **then**
    $Data \leftarrow Encrypted\_Data \oplus n$
  else if $EncAlg ==$ `AES` **then**
    $Data \leftarrow AES\_Decrypt(Encrypted\_Data, KeyDec)$
  else if $EncAlg ==$ `SHA`-based masking **then**
    $Data \leftarrow Encrypted\_Data \oplus SHA256(KeyDec)$
  end if
  return $Data$
end procedure

3.1.3. Blockchain network

The blockchain network serves as a decentralized ledger for the pharmaceutical supply chain, guaranteeing the accuracy and transparency of all information. The credentials and transaction history created throughout the supplier registration procedure are safely stored there. Only authorised parties are permitted to interact with certain data. In order to provide a reliable environment where every transaction is transparent, traceable, and incomparable, our system makes sure that all actions—including data uploads and verification requests—are safely recorded and verified.

3.1.4. Data addition and cncryption

Suppliers upload drug information to the SCM system, which then begins securely adding and encrypting the data for safe transmission. Algorithm 2 explains polymorphic encryption methods, which dynamically modify encryption schemes to improve data secrecy and integrity. The encryption phase begins when the SCM system initiates data uploading. For every data entry, a new pair of encryption and decryption keys ($KeyEn, KeyDec$) is generated. Simultaneously, a cryptographic procedure such as SHA-based masking, AES, or XOR is randomly selected from a predefined set. This random selection introduces unpredictability and enhances the system's resilience against pattern-based attacks. This encryption mechanism ensures that even if multiple suppliers transmit data simultaneously, the encryption pattern remains unique and adaptive to each session. For instance, if the XOR scheme is selected, a random number is generated and applied as a key to perform a bitwise transformation of the data.

In the case of AES, the data is encrypted using a symmetric block cipher with strong key-based encryption, whereas SHA-based masking applies the hash of the encryption key as a masking layer over the original data. The encrypted output, along with the relevant cryptographic metadata (such as the selected algorithm, decryption key, and any random values used), is then prepared for secure cloud storage. This polymorphic encryption method helps keep sensitive pharmaceutical data safe during both transmission and storage. Even if part of the encryption is compromised, the data stays protected. The use of random and changing encryption techniques makes it harder for attackers to break the system and improves the overall security of the decentralized SCM network.

3.1.5. Cloud storage integration

Cloud Storage Integration in the SCM system works together with the earlier steps of supplier registration and data encryption. After a sup-

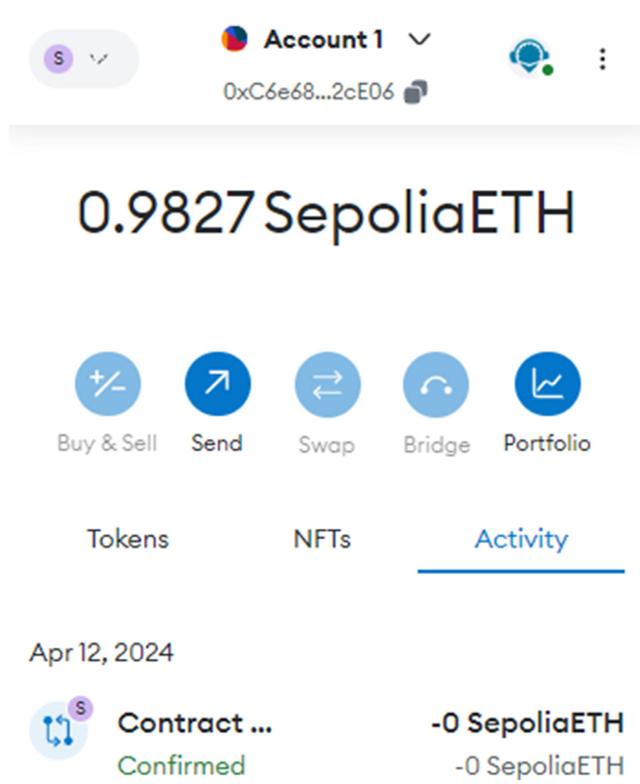

Fig. 4. Seamless smart contract deployment via MetaMask in Remix IDE, enabling authentication and transaction transfer to the Blockchain network.

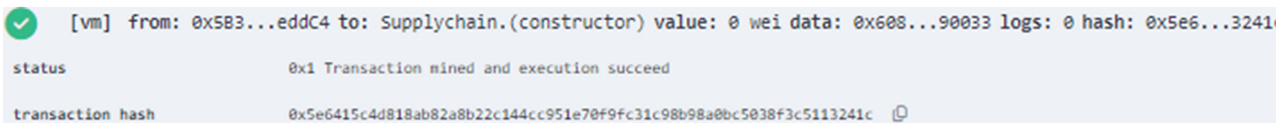

Fig. 5. Contract generation and data addition following the successful deployment of a smart contract in an SCM system, verified by MetaMask transaction confirmation.

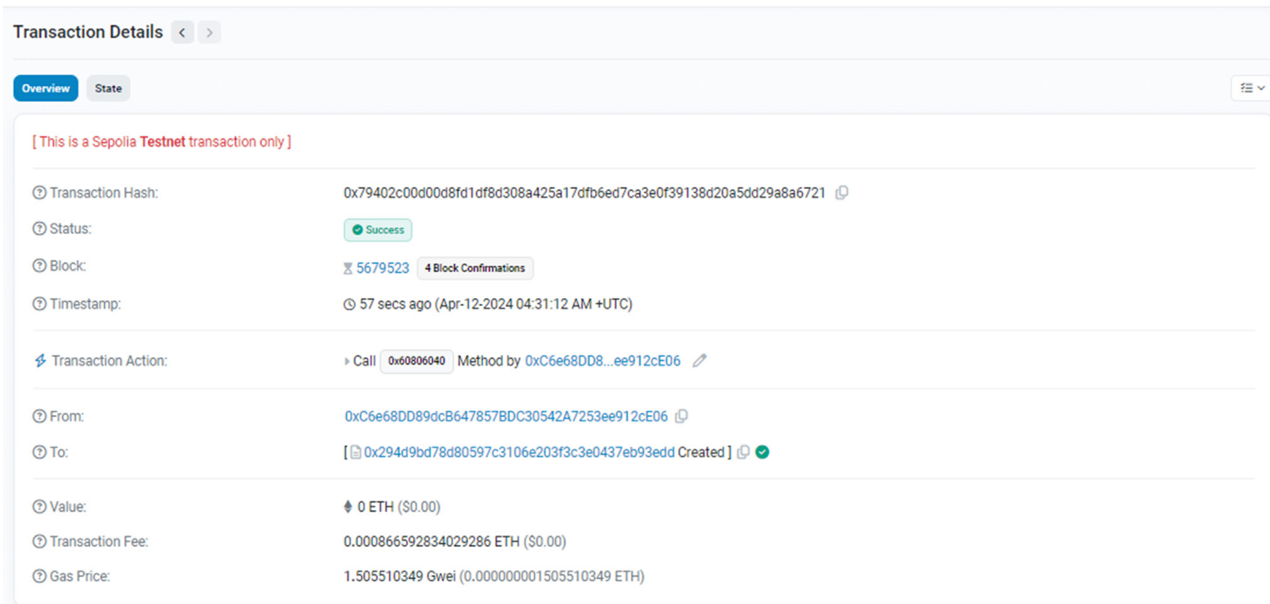

Fig. 6. The smart contract is successfully deployed, comprehensive transaction information is displayed on the test network, including transaction fees, hash values, and other specific information.

plier securely registers with cryptographic credentials, their drug data is encrypted using polymorphic techniques that dynamically change the encryption scheme for enhanced security. Each encrypted file is linked to its unique encryption key and algorithm details. This encrypted data is then safely stored in the cloud, ensuring it cannot be changed or accessed by unauthorized users. This process helps keep pharmaceutical data secure, organized, and tamper-proof throughout the supply chain.

3.1.6. Data retrieval and requests

When a retailer seeks to access product information, they first submit a request through the blockchain network. Upon receipt of the request, the blockchain network performs a validation process to authenticate the retailer's credentials, ensuring they possess the necessary authorization to retrieve the requested data. Once the blockchain network validates the retailer's access request, it returns the cloud storage address along with the required decryption metadata—namely, the decryption key, the algorithm identifier, and any random parameters. The SCM system then decrypts the data using the appropriate cryptographic method. If XOR encryption was used, the system applies the same random value to restore the original data. For AES encryption, the system performs AES decryption with the provided key. In the case of SHA-based masking, the system XORs the encrypted data with the SHA-256 hash of the decryption key. This process ensures that only authorized users can successfully decrypt and access the original product information.

4. Result and discussion

This section explores the efficiency of blockchain integration and cryptographic techniques in enhancing supply chain security and compares drug safety with the existing methodologies.

4.1. Environment configuration

The Remix IDE provides a comprehensive virtual environment for generating and executing smart contracts on the Ethereum network.

Smart contract integration is seamlessly managed within the Remix IDE platform. To deploy the contract in a public blockchain, authentication via MetaMask is necessary. The entire implementation process of the smart contract is facilitated within the Remix IDE environment. Figure 4 illustrates the transaction transfer to the blockchain network through the metamask extension tool, where Sepolia testnet network is used for the integration with a test ethereum blockchain network.

Fig. 5 illustrates that once the smart contract is successfully added on the Ethereum testnet by using MetaMask, the SCM contract is ready to be included to the blockchain. Mining algorithm is applied successfully resulting in a successful mining status and a valid hash number.

After confirmation of the Smart Contract transaction, its data will be added to the Ethereum platform, including details such as the transaction hash, transaction fee, gas price, and other relevant information shown in Fig. 6. In addition to these key components, several other details are recorded, including the timestamp, which indicates the exact date and time the transaction was processed. Additionally, the block number specifies the block in which the transaction was included and the gas price shows the total gas consumed by all transactions in the block, providing insight into network activity.

4.2. Deployed contract

The smart contract, "Supply Chain," facilitates the management of medicine and supplier details within a supply chain. It defines two main structs, "Medicine" and "Supplier," to encapsulate information such as medicine name, ID, description, manufacturer, quantity, expiration date, supplier name, ID, location, and contact information shown

Fig. 7. Smart contract "Supply Chain" before and after input, facilitating secure storage and access of medicine and supplier details in a decentralized supply chain management system on the Ethereum blockchain, incorporating set and get functions for data management.

in Fig. 7. The contract includes functions to set and retrieve these details, enabling users to store and access information about medicines and suppliers securely on the Ethereum blockchain. This contract serves as a foundation for building decentralized supply chain applications, ensuring transparency and traceability of products throughout their lifecycle.

4.3. Performance analysis

The research has found significant improvements in security, efficiency, and traceability with the following advancements,

- This model achieves a balance between security and computational efficiency, as evidenced by the moderate execution time for supplier registration, enabling practical scalability in real-world supply chains.
- By offloading decryption to an off-chain mechanism, the model significantly reduces on-chain gas costs and latency for data retrieval, improving system responsiveness without compromising data integrity.
- It has found unique security advantages over existing models to ensure efficient drug supply chain management.

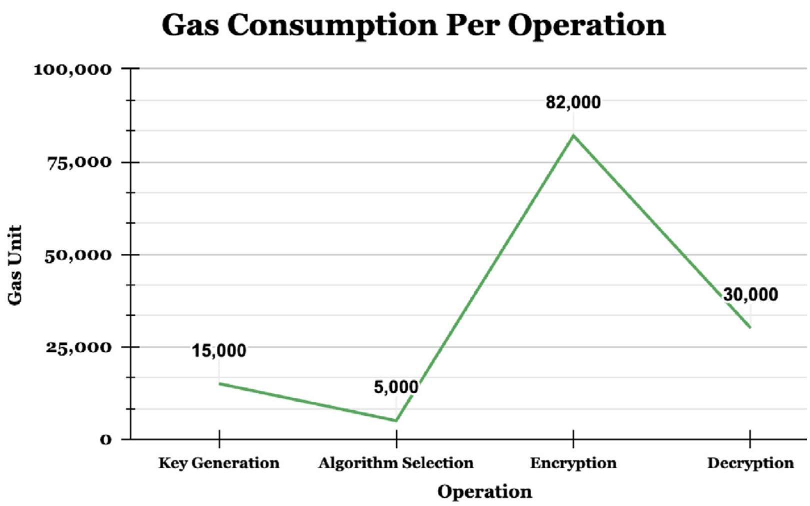

Fig. 8. This figure shows the gas costs of SCMapp's core operations: Key Generation, Algorithm Selection, Encryption, and Decryption. Encryption has the highest cost due to dynamic algorithm switching, while Algorithm Selection is the most efficient. The comparison illustrates the trade-off between security and efficiency in supply chain processes.

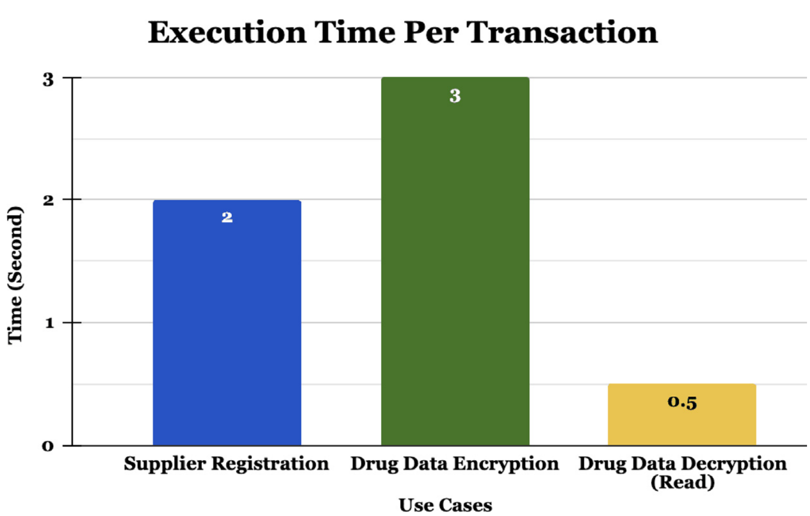

Fig. 9. This figure illustrates the execution time of SCMapp's key operations—Supplier Registration, Drug Data Encryption, and Decryption (Read). Encryption takes the longest (3s) due to computational overhead, while Decryption is fastest (0.5s) due to off-chain processing. The results highlight SCMapp's responsiveness and suitability for real-time supply chain management.

The performance of SCMapp is evaluated by measuring the gas costs of its core operations. These cost comparisons highlight the trade-offs between security and efficiency across the system's key processes.

The Fig. 8 provides a comparative overview of the computational cost, measured in gas units, for each major operation within the proposed blockchain-based Supply Chain Management application (SCMapp). The X-axis categorizes the key processes—namely, Key Generation, Algorithm Selection, Encryption, and Decryption—while the Y-axis represents the estimated gas consumption required for each operation. Among these, the Encryption phase incurs the highest gas cost, reaching approximately 82,000 units, due to the use of polymorphic techniques such as dynamic algorithm switching and secure key handling. Decryption consumes around 30,000 gas units, as it involves conditional logic for reversing encryption but without additional storage costs. Key Generation, at approximately 15,000 units, includes the creation of secure key pairs and identity-linked credentials. Algorithm Selection, being the simplest operation, has the lowest gas consumption at 5,000 units, reflecting lightweight randomness and control logic. This analysis shows that while encryption has a higher gas cost, the overall system achieves a strong balance between security and efficiency, making it well-suited for secure supply chain management.

Besides, it analyzes the execution time of its key operations to assess system responsiveness and real-time usability. Understanding how long each process takes helps validate the system's suitability for secure and efficient supply chain management.

The Fig. 9 clearly illustrates the execution time, measured in seconds, required for each key operation within the proposed Supply Chain Management Decentralized Application (SCMapp). Here X-axis represents the distinct blockchain-based processes performed—namely, Supplier Registration, Drug Data Encryption, and Drug Data Decryption (Read)—while the Y-axis indicates the execution time in seconds, reflecting the latency of each transaction from initiation to confirmation on the blockchain network.

The Supplier Registration operation demonstrates a moderate execution time of 2 s, representing the time needed to complete the process of adding a new participant to the supply chain. The Drug Data Encryption operation exhibits the highest execution time of 3 s, primarily due to the computational complexity of polymorphic encryption, which increases processing overhead to ensure stronger data protection against cryptanalysis.

In contrast, Drug Data Decryption (Read) achieves the fastest execution time of 0.5 s, owing to its off-chain design. While encrypted drug data are retrieved and decrypted off-chain (e.g., from a cloud server), only a reference pointer is accessed from the blockchain, resulting in minimal on-chain interaction and thus faster response time. The latency seen in the use cases shows better performance. Registration and encryption take a moderate amount of time because they involve secure blockchain and encryption steps. In contrast, reading data is much faster, which shows that the system works well for real-time supply chain management.

Table 3
Comparative analysis of the proposed model against existing solutions based on key features like smart contracts, cloud integration, encryption, traceability, and security. The proposed model ensures comprehensive coverage across all criteria.

Reference	Type	Year	Smart Contract	Cloud Integration	Encryption	Traceability	Security
Sharma et al. [69]	Blockchain	2024	√	✘	✘	√	√
Sumalatha et al. [70]	Blockchain	2024	√	✘	✘	√	√
Shruti et al. [71]	Encryption	2024	√	✘	√	✘	√
Talwandi et al. [72]	Blockchain, Cloud	2023	√	√	✘	✘	√
Deebak et al. [73]	Cloud	2023	✘	√	✘	✘	√
Proposed Model	Encryption, Blockchain, Cloud	-	√	√	√	√	√

Table 4
Vulnerability assessment comparing encryption diversity, tamper detection, and defenses against man-in-the-middle, Sybil, data poisoning, smart contract injection, and replay attacks across different system models, highlighting the security performance of the proposed architecture.

Aspect	Traditional System	Blockchain Based	Proposed System
Encryption Diversity	None or single algorithm	Single (e.g., AES)	Polymorphic (XOR, AES, SHA-masking randomized)
Tamper Detection	Weak	Strong (immutable logs)	Very Strong (hash + encrypted references)
Man-in-the-Middle Defense	Low	Medium (predictable patterns)	High (randomized encryption + secure metadata)
Sybil Attack	High risk (no node validation)	Moderate (requires consensus)	Low (registered actors, group keys, verified roles)
Data Poisoning	High (easy record injection)	Moderate (block validation only)	Low (encrypted + verified inputs per supplier node)
Storage Overhead	Low (but unstructured)	High (all data on-chain)	Efficient (off-chain storage, on-chain pointers only)
Gas Efficiency	Not applicable	Low (grows with operations)	High (optimized algorithm calls and metadata handling)
Smart Contract Injection	Not applicable	Medium (vulnerable to miswritten contracts)	Low (modular and validated encryption logic)
Replay Attack Resistance	Low	Moderate	High (non-reusable polymorphic encryption per txn)

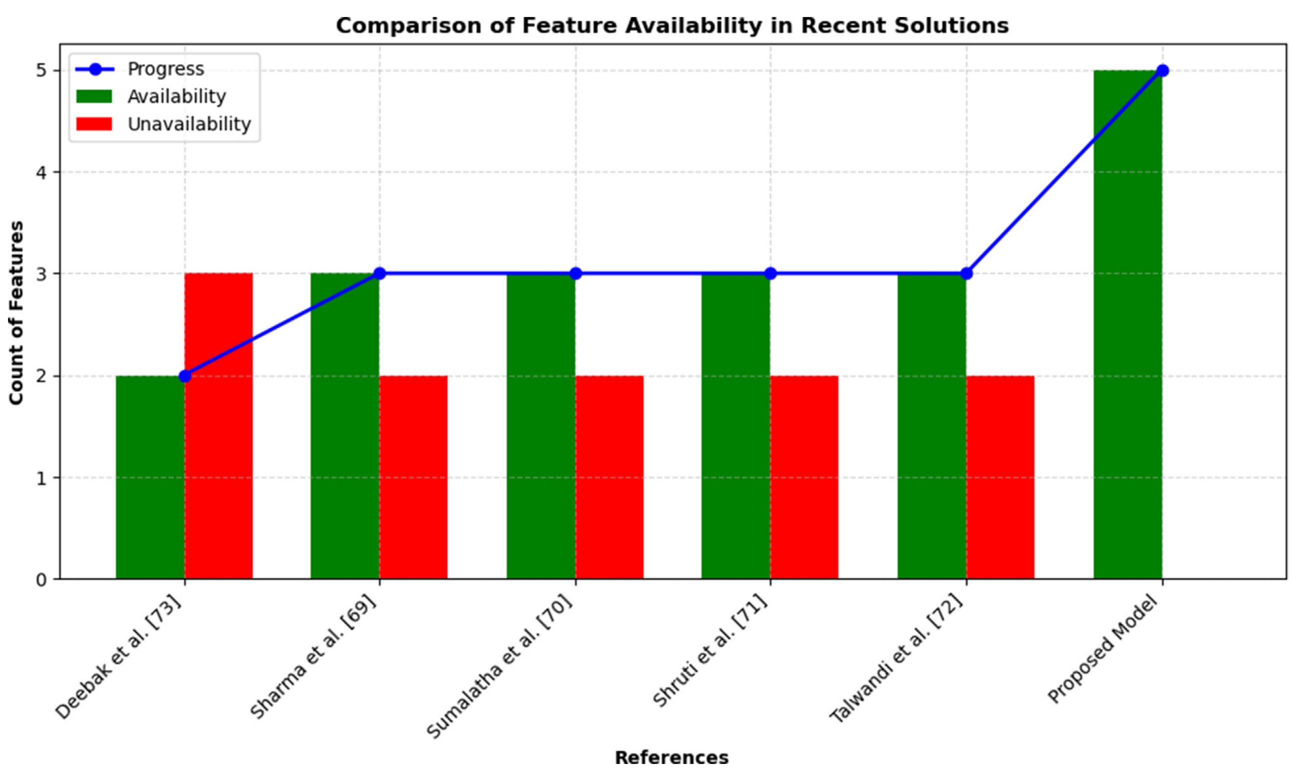

Fig. 10. The proposed model shows improved progress (blue line) with the highest number of available features (green bars) compared to other models. Red lines denote the lack of availability of essential feature. The Y-axis defines the sum of available features in a solution, and the X-axis shows the model.

4.4. Comparison

The Table 3 shows a comparison of different methods and solutions for managing drug supply chains. Our proposed model combines polymorphic encryption, blockchain, and cloud storage, and it stands out for its comprehensive security features. Unlike the other solutions, our model includes all the key features: smart contracts, cloud integration, encryption, traceability, and security. In contrast, other models fall short in several areas. For example the model developed by Sharma et al. [69] and Sumalatha et al. [70], lack cloud integration and encryption. These are essential for ensuring data security. Similarly, Shruti et al. [71] and Talwandi et al. [72] miss out on some crucial features like traceability. Which is important for monitoring the movement of drugs throughout the supply chain. This lack of tracking can make it challenging to ensure accountability of the supply management system. Deebak et al. [73] also falls short in terms of smart contracts and traceability.

Therefore, our proposed model offers a more secure and efficient solution for drug supply chain management. The progress has been demonstrated in Fig. 10.

4.5. Vulnerability risk analysis of SCMapp

Table 4 presents the results of our comparative assessment based on simulated transaction environments and vulnerability analysis. The proposed system, which integrates polymorphic encryption, blockchain immutability, and cloud-based storage, demonstrates significantly higher resilience to Sybil attacks, data poisoning, replay threats, and man-in-the-middle interception compared to both traditional and baseline blockchain models. The use of dynamic key generation and randomized algorithm selection reduces predictability in encryption, while offloading encrypted data to secure cloud storage improves gas efficiency and minimizes on-chain bloat. Overall, the proposed design achieves a better security-performance tradeoff and offers stronger operational scalability under real-world supply chain conditions.

5. Conclusion

A safe and effective method for managing drug supply chains is provided by the suggested Drug Supply Chain Management System. The proposed SCM model has been successfully tested on a blockchain network while enhancing security and improving accountability and traceability. It solves key problems in current systems by combining blockchain, cloud storage, and polymorphic encryption to protect data, keep it private, and make it transparent. Performance analysis confirms that key operations—such as supplier registration, encryption, and decryption—are carried out efficiently, supporting real-time responsiveness. In future, we will test this system in a real-world environment with a high volume of transactions. This will help validate the system's scalability and robustness under practical operational conditions. Although encryption is more computationally intensive due to advanced security features, it greatly strengthens data protection. Thus the system provides a strong balance between security and performance, ensuring operational reliability. Ongoing monitoring and proactive security measures further enhance its effectiveness. Overall, SCMapp not only protects the integrity of the drug supply chain but also improves transparency, efficiency, and stakeholder trust - making it a practical solution for real-world pharmaceutical supply chain operations.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Muammar Shahrear Famous: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Validation, Visualization, Writing – review & editing. **Samia Sayed:** Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Validation, Visualization, Writing – original draft. **Rashed Mazumder:** Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Validation, Visualization, Writing – original draft. **Risala T. Khan:** Conceptualization, Data curation, Formal analysis, Investigation, Validation, Visualization, Writing – original draft. **M. Shamim Kaiser:** Investigation, Methodology, Resources, Supervision, Writing – review & editing. **Mohammad Shahadat Hossain:** Investigation, Methodology, Project administration, Supervision, Writing – review & editing. **Karl Andersson:** Conceptualization, Investigation, Project administration, Supervision, Writing – review & editing. **Rahamatullah Khondoker:** Investigation, Methodology, Project administration, Validation, Writing – review & editing.

References

[1] X. Xu, N. Tian, H. Gao, H. Lei, Z. Liu, Z. Liu, A survey on application of blockchain technology in drug supply chain management, 2023, doi:10.1109/ICBDA57405.2023.10104779. Pages: 71
[2] L. Marchesi, Automatic generation of a blockchain-based drug supply chain management system, in: 2023 IEEE/ACM 6th International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), 2023, pp. 25–32, doi:10.1109/WETSEB59161.2023.00009. https://ieeexplore.ieee.org/document/10190815.
[3] D.H. Tanvir, R. Amin, A. Islam, M.S. Islam, M.M. Rashid, Blockchain interoperability for a reputation-based drug supply chain management, in: 2023 6th International Conference on Information Systems and Computer Networks (ISCON), 2023, pp. 1–6, doi:10.1109/ISCON57294.2023.10112196. https://ieeexplore.ieee.org/document/10112196. ISSN: 2832-143X
[4] Shalini S, Sheela S, Abhishek S, Bhavyashree P, Gunashree C, Rohan K S, An effective counterfeit medicine authentication system using blockchain and IoT, in: 2023 4th International Conference for Emerging Technology (INCET), 2023, pp. 1–5, doi:10.1109/INCET57972.2023.10170622. https://ieeexplore.ieee.org/document/10170622.
[5] A. Tahmasbzadeh, S. Kabirirad, A blockchain-based approach for data storage in drug supply chain, in: 2023 9th International Conference on Web Research (ICWR), 2023, pp. 335–341, doi:10.1109/ICWR57742.2023.10139084. https://ieeexplore.ieee.org/abstract/document/10139084.
[6] S. Sayed, M. Famous, S. Ahammad, T. Hossain, R. Khan, M. Kaiser, Toward distributed security based healthcare system, 2024, pp. 445–458, doi:10.1007/978-981-97-1923-5_34.
[7] L. Marchesi, Using Django framework and DLT for drug supply chain management, 2023, pp. 94–99, doi:10.1109/DAPPS57946.2023.00021.
[8] R.K. Jha, P. Alam, N. Priyadarshi, M.A. Ghazi, M.S. Bhargavi, Counterfeit drug prevention in pharma supply chain using blockchain technology, in: 2023 3rd International Conference on Intelligent Communication and Computational Techniques (ICCT), 2023, pp. 1–6, doi:10.1109/ICCT56969.2023.10076043. https://ieeexplore.ieee.org/document/10076043.
[9] S. Zaman, M.S. Kaiser, R. Tasin Khan, M. Mahmud, Towards SDN and blockchain based IoT countermeasures: a survey, in: 2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI), 2020, pp. 1–6, doi:10.1109/STI50764.2020.9350392. https://ieeexplore.ieee.org/document/9350392.
[10] K. Abbas, M. Afaq, T.A. Khan, W.-C. Song, A blockchain and machine learning-based drug supply chain management and recommendation system for smart pharmaceutical industry, in: 2023 Semantic Scholar, https://www.semanticscholar.org/paper/A-Blockchain-and-Machine-Learning-Based-Drug-Supply-Abbas-Afaq/5beff11072de25e9be72bd02acc2215a254566e4.
[11] D. Alsagheer, L. Xu, W. Shi, Decentralized machine learning governance: overview, opportunities, and challenges, in: 2023 IEEE Xplore, https://ieeexplore.ieee.org/document/10238468.
[12] V. Charles, A. Emrouznejad, T. Gherman, et al., A critical analysis of the integration of blockchain and artificial intelligence for supply chain, Ann. Oper. Res. 327 (1) (2023) 7–47, doi:10.1007/s10479-023-05169-w.
[13] R. Pathak, V. Gaur, H. Sankrityayan, Gogtay, Jaideep, Tackling counterfeit drugs: the challenges and possibilities, in: 2023 PMC, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10184969/.
[14] V. Ahmadi, S. Benjelloun, M. El Kik, T. Sharma, H. Chi, W. Zhou, Drug governance: IoT-based blockchain implementation in the pharmaceutical supply chain, in: 2020 Sixth International Conference on Mobile And Secure Services (MobiSecServ), 2020, pp. 1–8, doi:10.1109/MobiSecServ48690.2020.9042950. https://ieeexplore.ieee.org/document/9042950. ISSN: 2640-558X
[15] R. Singh, A.D. Dwivedi, G. Srivastava, Internet of things based blockchain for temperature monitoring and counterfeit pharmaceutical prevention, in: 2020 Sensor, https://www.mdpi.com/1424-8220/20/14/3951.
[16] X. Chen, C. He, Y. Chen, Z. Xie, et al., Internet of things (IoT)—blockchain-enabled pharmaceutical supply chain resilience in the post-pandemic era, Front. Eng. Manag. 10 (1) (2023) 82–95, doi:10.1007/s42524-022-0233-1.
[17] A. Altigani, S. Hasan, B. Barry, S. Naserelden, M.A. Elsadig, H.T. Elshoush, et al., A polymorphic advanced encryption standard - a novel approach, IEEE Access 9 (2021) 20191–20207, doi:10.1109/ACCESS.2021.3051556. Conference Name: IEEE Access
[18] D.D. Booher, B. Cambou, A.H. Carlson, C. Philabaum, Dynamic key generation for polymorphic encryption: 9th IEEE Annual Computing and Communication Workshop and Conference, CCWC 2019, in: 2019 IEEE 9th Annual Computing and Communication Workshop and Conference, CCWC 2019, Publisher: Institute of Electrical and Electronics Engineers Inc., 2019, pp. 482–487, doi:10.1109/CCWC.2019.8666500. http://www.scopus.com/inward/record.url?scp=85063904703.
[19] Y. Meng, J. Li, Data sharing mechanism of sensors and actuators of industrial IoT based on blockchain-assisted identity-based cryptography, 2021 Sensor, https://www.mdpi.com/1424-8220/21/18/6084.
[20] K.-A. Shim, Y. An, Cryptanalysis of lattice-based blind signature and blind ring signature schemes, IEEE Access 9 (2021) 134427–134434, doi:10.1109/ACCESS.2021.3113938. Conference Name: IEEE Access
[21] E. Simion, Encapsulating secrets using lockable obfuscation and a RMERS-based public key encryption, Sustainability 14 (18) (2022) 11412, doi:10.3390/su141811412. Number: 18 Publisher: Multidisciplinary Digital Publishing Institute
[22] J. Xie, W. Zhao, H. Lee, D.B. Roy, X. Zhang, et al., Hardware circuits and systems design for post-quantum cryptography—A tutorial brief, IEEE Trans. Circuits Syst. II Express Briefs 71 (3) (2024) 1670–1676, doi:10.1109/TCSII.2024.3357836. Conference Name: IEEE Transactions on Circuits and Systems II: Express Briefs

[23] S. Kim, Optimized SeaSign for enhanced efficiency, IEEE Access PP (2024), doi:10.1109/ACCESS.2024.3360297. 1–1
[24] Y. Merrad, M.H. Habaebi, M.R. Islam, T.S. Gunawan, M. Mesri, et al., Robust decentralized proof of location for blockchain energy applications using game theory and random selection, Sustainability 14 (10) (2022), doi:10.3390/su14106123.
[25] M. Dashtizadeh, F. Meskaran, D. Tan, et al., A secure blockchain-based pharmaceutical supply chain management system: traceability and detection of counterfeit Covid-19 vaccines, in: 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon), 2022, pp. 1–5, doi:10.1109/MysuruCon55714.2022.9972646. https://ieeexplore.ieee.org/document/9972646.
[26] A. Musamih, R. Jayaraman, K. Salah, H.R. Hasan, I. Yaqoob, Y. Al-Hammadi, Blockchain-based solution for distribution and delivery of COVID-19 vaccines, IEEE Access 9 (2021) 71372–71387, doi:10.1109/ACCESS.2021.3079197.
[27] A. Musamih, R. Jayaraman, K. Salah, H.R. Hasan, I. Yaqoob, Y. Al-Hammadi, Blockchain-based solution for the administration of controlled medication, IEEE Journals & Magazine, IEEE Xplore, 2021b, https://ieeexplore.ieee.org/document/9581053.
[28] M. Mohit, S. Kaur, M. Singh, et al., Design and implementation of transaction privacy by virtue of ownership and traceability in blockchain based supply chain, Cluster Comput. 25 (3) (2022) 2223–2240, doi:10.1007/s10586-021-03425-x.
[29] P. Saindane, Y. Jethani, P. Mahtani, C. Rohra, P. Lund, Blockchain: a solution for improved traceability with reduced counterfeits in supply chain of drugs, in: 2020 International Conference on Electrotechnical Complexes and Systems (ICOECS), 2020, pp. 1–5, doi:10.1109/ICOECS50468.2020.9278412. https://ieeexplore.ieee.org/document/9278412.
[30] D. Marbouh, T. Abbasi, F. Maasmi, I.A. Omar, M.S. Debe, K. Salah, R. Jayaraman, S. Ellahham, et al., Blockchain for COVID-19: review, opportunities, and a trusted tracking system, Arabian J. Sci. Eng. 45 (12) (2020) 9895–9911, doi:10.1007/s13369-020-04950-4.
[31] M. Debe, K. Salah, R. Jayaraman, J. Arshad, et al., Blockchain-based verifiable tracking of resellable returned drugs, IEEE Access 8 (2020) 205848–205862, doi:10.1109/ACCESS.2020.3037363. Conference Name: IEEE Access
[32] S.E. Chang, Y. Chen, When Blockchain Meets supply chain: a systematic literature review on current development and potential applications, IEEE Journals & Magazine, IEEE Xplore, 2020, https://ieeexplore.ieee.org/document/9047881.
[33] Y. Shah, Y. Verma, U. Sharma, A. Sampat, V. Kulkarni, Supply chain for safe & timely distribution of medicines using blockchain & machine learning, in: 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT), 2023, pp. 1123–1129, doi:10.1109/ICSSIT55814.2023.10061049. https://ieeexplore.ieee.org/document/10061049. ISSN: 2832-3017
[34] M. Sahoo, S.S. Singhar, B. Nayak, B.K. Mohanta, A blockchain based framework secured by ecdsa to curb drug counterfeiting, in: 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2019, pp. 1–6, doi:10.1109/ICCCNT45670.2019.8944772. https://ieeexplore.ieee.org/document/8944772.
[35] F. Jamil, L. Hang, K. Kim, D.-H. Kim, A Novel medical blockchain model for drug supply chain integrity management in a smart hospital, Semantic Scholar, 2019, https://www.semanticscholar.org/paper/A-Novel-Medical-Blockchain-Model-for-Drug-Supply-in-Jamil-Hang/c113293f1ec69583310186df62320dee2c903096.
[36] H.L. Pham, T.H. Tran, Y. Nakashima, practical anti-counterfeit medicine management system based on blockchain technology, in: 2019 4th Technology Innovation Management and Engineering Science International Conference (TIMES-iCON), 2019, pp. 1–5, doi:10.1109/TIMES-iCON47539.2019.9024674. https://ieeexplore.ieee.org/document/9024674.
[37] R. Jayaraman, F. AlHammadi, M.C.E. Simsekler, Managing product recalls in healthcare supply chain, in: 2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), 2018, pp. 293–297, doi:10.1109/IEEM.2018.8607403. https://ieeexplore.ieee.org/document/8607403. ISSN: 2157-362X
[38] Q. He, H. He, A novel method to enhance sustainable systems security in cloud computing based on the combination of encryption and data mining, Sustainability 13 (1) (2021) 101, doi:10.3390/su13010101. Number: 1 Publisher: Multidisciplinary Digital Publishing Institute
[39] V. Mani, M. Prakash, W.-C. Lai, et al., Cloud-based blockchain technology to identify counterfeits, J. Cloud Comput. 11 (2022), doi:10.1186/s13677-022-00341-2.
[40] Z. Xu, M. Luo, C. Peng, Q. Feng, Sanitizable signature scheme with privacy protection for electronic medical data sharing, Cyber Secur. Appl. 1 (2023) 100018, doi:10.1016/j.csa.2023.100018.
[41] M. Rahaman, F. Tabassum, V. Arya, R. Bansal, Secure and sustainable food processing supply chain framework based on Hyperledger Fabric technology, Cyber Secur. Appl. 2 (2024) 100045, doi:10.1016/j.csa.2024.100045.
[42] A. Alqudhaibi, M. Albarrak, S. Jagtap, N. Williams, K. Salonitis, Securing industry 4.0: assessing cybersecurity challenges and proposing strategies for manufacturing management, Cyber Secur. Appl. 3 (2025) 100067, doi:10.1016/j.csa.2024.100067.
[43] M. Javaid, A. Haleem, R.P. Singh, R. Suman, Towards insighting cybersecurity for healthcare domains: a comprehensive review of recent practices and trends, Cyber Secur. Appl. 1 (2023) 100016, doi:10.1016/j.csa.2023.100016.
[44] K. Agrawal, M. Aggarwal, S. Tanwar, A. Alabdulatif, Adoption of blockchain to develop a deployable secure healthcare solution: an analysis, Cyber Secur. Appl. (2024) 100060, doi:10.1016/j.csa.2024.100060.
[45] V. Crossland, C. Dellwo, G. Bashar, G.G. Dagher, et al., Janus: toward preventing counterfeits in supply chains utilizing a multi-quorum blockchain, Blockchain Res. Appl. 4 (4) (2023) 100157, doi:10.1016/j.bcra.2023.100157.
[46] M. Javaid, A. Haleem, R. Pratap Singh, S. Khan, R. Suman, Blockchain technology applications for Industry 4.0: a literature-based review, Blockchain Res. Appl. 2 (4) (2021) 100027, doi:10.1016/j.bcra.2021.100027.
[47] S. Cao, M. Foth, W. Powell, T. Miller, M. Li, et al., A blockchain-based multisignature approach for supply chain governance: a use case from the Australian beef industry, Blockchain Res. Appl. 3 (4) (2022) 100091, doi:10.1016/j.bcra.2022.100091.
[48] P. Bottoni, C. Di Ciccio, R. Pareschi, D. Tortola, N. Gessa, G. Massa, Blockchain-as-a-Service and blockchain-as-a-partner: implementation options for supply chain optimization, Blockchain Res. Appl. 4 (2) (2023) 100119, doi:10.1016/j.bcra.2022.100119.
[49] A. Vaghani, K. Sood, S. Yu, Security and QoS issues in blockchain enabled next-generation smart logistic networks: a tutorial, Blockchain Res. Appl. 3 (3) (2022) 100082, doi:10.1016/j.bcra.2022.100082.
[50] D. Adam, D.B. Matellini, A. Kaparaki, et al., Benefits for the bunker industry in adopting blockchain technology for dispute resolution, Blockchain Res. Appl. 4 (2) (2023) 100128, doi:10.1016/j.bcra.2023.100128.
[51] C. Regueiro, A. Gómez-Goiri, N. Pedrosa, C. Semertzidis, E. Iturbe, J. Mansell, Blockchain-based refurbishment certification system for enhancing the circular economy, Blockchain Res. Appl. 5 (1) (2024) 100172, doi:10.1016/j.bcra.2023.100172.
[52] P.S. Akshatha, S.M. Dilip Kumar, MQTT and blockchain sharding: an approach to user-controlled data access with improved security and efficiency, Blockchain Res. Appl. 4 (4) (2023) 100158, doi:10.1016/j.bcra.2023.100158.
[53] H. Chen, X. Luo, L. Shi, Y. Cao, Y. Zhang, Security challenges and defense approaches for blockchain-based services from a full-stack architecture perspective, Blockchain Res. Appl. 4 (3) (2023) 100135, doi:10.1016/j.bcra.2023.100135.
[54] C. Allenbrand, Smart contract-enabled consortium blockchains for the control of supply chain information distortion, Blockchain Res. Appl. 4 (3) (2023) 100134, doi:10.1016/j.bcra.2023.100134.
[55] A. Sarfaraz, R.K. Chakrabortty, D.L. Essam, The implications of blockchain-coordinated information sharing within a supply chain: a simulation study, Blockchain Res. Appl. 4 (1) (2023) 100110, doi:10.1016/j.bcra.2022.100110.
[56] L. Cui, Z. Xiao, F. Chen, H. Dai, J. Li, Protecting vaccine safety: an improved, blockchain-based, storage-efficient scheme, IEEE Journals & Magazine, IEEE Xplore, 2022, https://ieeexplore.ieee.org/document/9756664.
[57] I.A. Omar, M. Debe, R. Jayaraman, K. Salah, M. Omar, J. Arshad, et al., Blockchain-based supply chain traceability for COVID-19 personal protective equipment, Comput. Ind. Eng. 167 (2022) 107995, doi:10.1016/j.cie.2022.107995.
[58] H. Amoozad Mahdiraji, F. Yaftiyan, A. Abbasi-Kamardi, J.A. Garza-Reyes, et al., Investigating potential interventions on disruptive impacts of industry 4.0 technologies in circular supply chains: evidence from SMEs of an emerging economy, Comput. Ind. Eng. 174 (2022) 108753, doi:10.1016/j.cie.2022.108753.
[59] A. Kumar, V. Mani, V. Jain, H. Gupta, V.G. Venkatesh, Managing healthcare supply chain through artificial intelligence (AI): a study of critical success factors - ScienceDirect, 2022, https://www.sciencedirect.com/science/article/pii/S0360835222008038.
[60] L. Liu, W. Song, Y. Liu, et al., Leveraging digital capabilities toward a circular economy: Reinforcing sustainable supply chain management with Industry 4.0 technologies, Comput. Ind. Eng. 178 (2023) 109113, doi:10.1016/j.cie.2023.109113.
[61] J. Li, D. Han, Z. Wu, J. Wang, K.-C. Li, A. Castiglione, A novel system for medical equipment supply chain traceability based on alliance chain and attribute and role access control - ScienceDirect, 2023, https://www.sciencedirect.com/science/article/abs/pii/S0167739X22004411.
[62] P. Chithaluru, F. Al-Turjman, R. Dugyala, T. Stephan, M. Kumar, J.S. Dhatterwal, RETRACTED: an enhanced consortium blockchain diversity mining technique for IoT metadata aggregation, Future Gener. Comput. Syst. 152 (2024) 239–253, doi:10.1016/j.future.2023.10.020.
[63] S. Bistarelli, F. Faloci, P. Mori, *-chain: a framework for automating the modeling of blockchain based supply chain tracing systems - ScienceDirect, 2023, https://www.sciencedirect.com/science/article/pii/S0167739X23002625.
[64] S. Zaman, M. Khandaker, R. Khan, F. Tariq, K.-K. Wong, et al., Thinking out of the blocks: holochain for distributed security in IoT healthcare, IEEE Access 10 (2022), doi:10.1109/ACCESS.2022.3163580. 1–1
[65] S. Zaman, K. Alhazmi, M.A. Aseeri, M.R. Ahmed, R.T. Khan, M.S. Kaiser, M. Mahmud, et al., Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey, IEEE Access 9 (2021) 94668–94690, doi:10.1109/ACCESS.2021.3089681. Conference Name: IEEE Access
[66] A. El Koshiry, E. Eliwa, T. Abd El-Hafeez, M.Y. Shams, Unlocking the power of blockchain in education: an overview of innovations and outcomes, Blockchain Res. Appl. 4 (4) (2023) 100165, doi:10.1016/j.bcra.2023.100165.
[67] V. Kumar, S.K. Das, Enhancing security in IIoT: RFID authentication protocol for edge computing and blockchain-enabled supply chain, Cyber Secur. Appl. 3 (2025) 100087, doi:10.1016/j.csa.2025.100087.
[68] C. Rupa, G.S. Varshitha, D. Divya, T.R. Gadekallu, M.J. Piran, et al., Blockchain-based DApp for drug supply chain with ai-driven drug recommender system, IEEE Consum. Electron. Mag. (2025) 1–6, doi:10.1109/MCE.2025.3536326.
[69] D. Sharma, A. Singhal, K. Singh, P. Singh, Fake/Counterfeit medical product identification using blockchain & QR Code, 2024, doi:10.1109/ICDT61202.2024.10489506. Pages: 1026
[70] M.R. Sumalatha, D. Raghuraman, S. S, M. V, Secured blockchain technology for medical supply chain (SB-MSC), in: 2024 International Conference on Advances in Data Engineering and Intelligent Computing Systems (ADICS), 2024, pp. 1–6, doi:10.1109/ADICS58448.2024.10533582. https://ieeexplore.ieee.org/document/10533582.
[71] S. Shruti, B. Alapatt, J. George, et al., MediCrypt: a model with symmetric encryption for blockchain enabled healthcare data protection, in: 2024 IEEE International Conference on Contemporary Computing and Communications (InC4), vol. 1, 2024, pp. 1–6, doi:10.1109/InC460750.2024.10649142. https://ieeexplore.ieee.org/document/10649142/keywords.

[72] N.S. Talwandi, N. Kaur Walia, Enhancing security of cloud computing transaction using blockchain, in: 2023 International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT), 2023, pp. 1133–1139, doi:10.1109/ICAICCIT60255.2023.10466075. https://ieeexplore.ieee.org/abstract/document/10466075.

[73] B.D. Deebak, S.O. Hwang, Healthcare Applications using blockchain with a cloud-assisted decentralized privacy-preserving framework, IEEE Trans. Mob. Comput. 23 (5) (2024) 5897–5916, doi:10.1109/TMC.2023.3315510. Conference Name: IEEE Transactions on Mobile Computing