WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Pharmacy Fraud Detection and Security Using Block Chain

Prof. Prashant Govardhan[1], Aniket Kokate[2], Ritesh Lolusare[3], Rupak Ganvir[4], Ishank Thakre[5], Priyanka Sarode[6]

[1]Computer Science & Engineering, PCE, Nagpur, Maharashtra, India
[2]Computer Science & Engineering, PCE, Nagpur, Maharashtra, India Aniketkokate2110@gmail.com
[3]Computer Science & Engineering, PCE, Nagpur, Maharashtra, India lolusareritesh@gmail.com
[4]Computer Science & Engineering, PCE, Nagpur, Maharashtra, India
[5]Computer Science & Engineering, PCE, Nagpur, Maharashtra, India
[6]Computer Science & Engineering, PCE, Nagpur, Maharashtra, India

ABSTRACT–

Pharmacy fraud is a significant problem in the healthcare industry that can lead to financial losses, compromised patient safety, and even loss of life. To address this issue, the use of blockchain technology has gained attention as a potential solution due to its inherent security features. This paper proposes a pharmacy fraud detection and security system using blockchain technology. The system employs a smart contract to ensure that all transactions are recorded in a tamper-proof and transparent manner, enabling fraud detection in real-time. Additionally, the system uses a permissioned blockchain to control access to the network and ensure data privacy. The proposed system offers a reliable, secure, and efficient solution to combat pharmacy fraud while safeguarding patient information.

Keywords- Pharmacy Fraud, Blockchain, Cryptography QR (Quick Response) Code, Fraud Detection etc.

I. INTRODUCTION

Pharmacy fraud is a growing concern in the healthcare industry, causing significant harm to patients and financial losses for healthcare providers. Fraudulent activities such as counterfeit drugs, prescription forgery, and insurance fraud can compromise patient safety and negatively impact the reputation of healthcare organizations. Fortunately, blockchain technology has emerged as a promising solution to combat this issue.

Blockchain technology can create a decentralized and immutable ledger of transactions, making it difficult for fraudsters to tamper with the data. According to Vigna and Casey's study (2015), blockchain technology can create a transparent and secure platform for recording and sharing information that can prevent fraudulent activities. By using blockchain technology, every transaction is recorded, timestamped, and validated by the network, making it challenging to modify or manipulate the data. This transparency can help detect fraudulent activities and mitigate the risk of fraud in the pharmacy industry.

In addition to detecting fraud, blockchain technology can improve medication safety by enabling faster and more accurate identification of potential safety concerns. Liu et al. (2019) proposed a blockchain-based system for adverse drug reaction reporting that can help healthcare providers and regulatory agencies to identify and address safety issues in real-time. Pharmacy fraud is a significant problem in the healthcare industry that can lead to financial losses, compromised patient safety, and even loss of life. To address this issue, the use of blockchain technology has gained attention as a potential solution due to its inherent security features. This paper proposes a pharmacy fraud detection and security system using blockchain technology. By using blockchain technology to record and share adverse drug reactions, the healthcare industry can take prompt action to address safety concerns and prevent harm to patients.

Patient privacy and confidentiality can also be ensured through blockchain technology, as demonstrated in a study by Lu et al. (2020), which proposes a blockchain-based healthcare data sharing platform that allows patients to control access to their health records while still enabling healthcare providers to access necessary information. Furthermore, blockchain technology can automate pharmacy-related transactions, minimizing the potential for errors and fraud. A smart contract-based pharmacy management system that automates drug dispensing and inventory management is proposed in a research paper by Yaqoob et al. (2021).

Overall, blockchain technology offers promising solutions for detecting pharmacy fraud, improving medication safety, protecting patient privacy, and automating pharmacy-related transactions. With further research and development, blockchain technology is expected to gain wider adoption in the pharmacy industry.

The use of blockchain technology has emerged as a promising solution for the pharmacy industry to address the challenges of fraud, medication safety, and patient privacy. The decentralized and secure platform provided by blockchain technology has the potential to revolutionize the way healthcare providers manage patient care and medication dispensing.

One of the most significant advantages of blockchain technology in pharmacy is its ability to detect and prevent fraud. The transparency provided by blockchain ensures that every transaction is recorded and validated by the network, making it difficult for fraudsters to tamper with the data. This increased transparency can help detect fraudulent activities and mitigate the risk of fraud in the pharmacy industry.

Furthermore, blockchain technology can improve medication safety by enabling faster and more accurate identification of potential safety concerns. By using blockchain technology to record and share adverse drug reactions, healthcare providers can take prompt action to address safety concerns and prevent harm to patients.

Patient privacy and confidentiality are also critical concerns in the healthcare industry. The use of a blockchain-based healthcare data sharing platform can allow patients to control access to their health records while still enabling healthcare providers to access necessary information. Also, the use of smart contracts on the blockchain can automate pharmacy-related transactions, reducing the potential for errors and fraud. This automation can simplify the medication dispensing process, minimize the risk of errors, and reduce costs.

Blockchain technology is known for its robust security features, which make it an attractive solution for industries that require secure and tamper-proof data storage and sharing. The decentralized nature of the blockchain network, along with its cryptographic algorithms, ensures that data stored on the blockchain is secure and cannot be modified by unauthorized parties.

One of the key features of blockchain security is its immutability. Once data is recorded on the blockchain, it cannot be altered or deleted without the consensus of the network participants. This ensures that the data remains tamper-proof and resistant to attacks. Another security feature of blockchain is its use of cryptographic algorithms to secure data. Transactions on the blockchain network are verified through complex algorithms that use cryptographic keys to ensure that only authorized parties can access the data. This helps to prevent unauthorized access to sensitive information and ensures the integrity of the data. Additionally, blockchain networks are decentralized, meaning that data is stored across multiple nodes on the network. This distributed architecture makes it difficult for attackers to compromise the network, as they would need to gain control of a majority of the nodes to do so. This makes blockchain networks highly resilient to attacks, ensuring the security of the data stored on the network.

However, despite the robust security features of blockchain, it is not immune to all forms of attack. For example, attacks on individual nodes or endpoints can still compromise the security of the network. Additionally, if a network is controlled by a small group of actors, they may be able to collude to compromise the security of the network.

In conclusion, blockchain technology has the potential to transform the pharmacy industry by providing a secure and transparent platform for recording and sharing information. By using blockchain technology to combat fraud, improve medication safety, protect patient privacy, and automate pharmacy-related transactions, the healthcare industry can improve patient care while reducing costs and mitigating risk. With further research and development, blockchain technology is expected to gain wider adoption in the pharmacy industry.

II. LITERATURE SURVEY

From [1], by S. S. Hussain et al. (2019) proposes a blockchain-based framework to enhance the security and privacy of healthcare data in cloud-based systems. The paper highlights the challenges of healthcare data security in cloud-based systems and the potential of blockchain technology in addressing these challenges. The proposed framework uses blockchain to ensure secure data sharing, access control, and privacy-preserving data sharing. It also prevents unauthorized access, tampering, and data breaches.

The authors suggest that the proposed framework can provide an effective solution to the challenges of healthcare data security in cloud-based systems. They also highlight the benefits of using blockchain, such as decentralization, transparency, immutability, and consensus. The proposed framework can be used in different healthcare applications, such as electronic health records, medical imaging, and patient monitoring systems. The authors suggest that the implementation of the proposed framework requires further research and development to address the scalability and interoperability issues.

From [2], by J. Choi et al. (2019) presents a blockchain-based framework for enhancing the security and privacy of healthcare applications. The paper highlights the challenges of healthcare data security in healthcare applications and the potential of blockchain technology in addressing these challenges. The proposed framework uses blockchain to ensure secure data sharing, access control, and privacy-preserving data sharing. It also prevents unauthorized access, tampering, and data breaches.

The authors suggest that the proposed framework can provide an effective solution to the challenges of healthcare data security in healthcare applications. They also highlight the benefits of using blockchain, such as decentralization, transparency, immutability, and consensus. The proposed framework can be used in different healthcare applications, such as electronic health records, medical imaging, and patient monitoring systems. The authors suggest that the implementation of the proposed framework requires further research and development to address the scalability and interoperability issues.

From [3], by S. S. Hussain et al. (2019) proposes a blockchain-based decentralized control system for healthcare systems. The paper highlights the challenges of healthcare data security in centralized healthcare systems and the potential of blockchain technology in addressing these challenges. The

proposed system uses blockchain to ensure secure data sharing, access control, and privacy-preserving data sharing. It also prevents unauthorized access, tampering, and data breaches.

The authors suggest that the proposed system can provide an effective solution to the challenges of healthcare data security in centralized healthcare systems. They also highlight the benefits of using blockchain, such as decentralization, transparency, immutability, and consensus. The proposed system can be used in different healthcare applications, such as electronic health records, medical imaging, and patient monitoring systems. The authors suggest that the implementation of the proposed system requires further research and development to address the scalability and interoperability issues.

From [4], by Y. Zhang, X. Xu, Y. Ren, and H. Guo proposes a blockchain-based framework to provide secure and privacy-preserving healthcare information sharing. The paper highlights that the traditional centralized approach to healthcare information management is susceptible to cyber-attacks, breaches, and unauthorized access, which can result in significant consequences, such as identity theft, financial loss, and health risks. Therefore, the authors propose a blockchain-based framework that utilizes a distributed access control mechanism to safeguard sensitive healthcare information from unauthorized access. Smart contracts are employed to automate access control and enforce predefined policies to ensure data sharing is compliant with regulatory requirements. Furthermore, the framework utilizes privacy-preserving mechanisms such as homomorphic encryption and zero-knowledge proof to enable secure and privacy-preserving data sharing. The paper also provides a comprehensive evaluation of the proposed framework through experiments, and the results show that the framework can achieve efficient and secure healthcare information sharing.

From [5], "A Blockchain-Based Approach to Enhancing the Security and Privacy of Electronic Health Records" by A. V. D. Perera, D. N. Ranasinghe, and X. Li proposes a blockchain-based approach to enhance the security and privacy of electronic health records (EHRs). The paper argues that the conventional approach to EHR management, which relies on centralized systems, is not secure and can be prone to various cyber threats. Therefore, the authors propose a blockchain-based approach that employs a private blockchain to store EHRs, which are encrypted to ensure confidentiality. A consensus mechanism is utilized to ensure that EHRs are tamper-proof and immutable. Smart contracts are used to automate access control and enforce data sharing policies. Additionally, the approach utilizes differential privacy to provide privacy-preserving data sharing. The paper also evaluates the proposed approach through simulations, and the results demonstrate its effectiveness in ensuring secure and privacy-preserving EHR sharing.

From [6], "A Blockchain-Based Electronic Health Record System for Healthcare Services" by S. S. Lee, S. Kim, and K. Kim proposes a blockchain-based electronic health record (EHR) system for healthcare services. The paper argues that traditional EHR systems are often siloed, inefficient, and lack interoperability. Therefore, the authors propose a blockchain-based approach that utilizes a private blockchain to store EHRs, which are encrypted to ensure confidentiality. A consensus mechanism is employed to ensure that EHRs are tamper-proof and immutable. Smart contracts are used to automate access control and enforce data sharing policies. The proposed system offers advantages such as scalability, interoperability, and decentralization. The paper evaluates the proposed system through simulations and experiments, and the results demonstrate its effectiveness in ensuring secure and efficient healthcare information sharing. Additionally, the authors suggest that the proposed system can help address the challenges associated with traditional EHR systems, such as fragmentation, duplication, and inconsistency.

[7] by J. M. Ahram and E. O. H. El-Masri, This paper proposes a blockchain-based solution to promote patient-driven interoperability in healthcare systems. The authors argue that the current lack of interoperability among healthcare systems hinders effective patient care and treatment. The blockchain-based solution enables secure sharing of patient data across multiple healthcare providers and institutions, allowing for better coordination of care and improved patient outcomes. The system also offers greater transparency and control for patients over their personal health information.

The authors propose a four-layered architecture for the blockchain-based solution, which includes a data layer, identity layer, smart contract layer, and user interface layer. The data layer stores patient health information, while the identity layer ensures secure identification of patients and healthcare providers. The smart contract layer facilitates automated transactions among healthcare providers, while the user interface layer enables patients to access and manage their health information. The proposed solution has several advantages over traditional healthcare systems, including improved data security, reduced data fragmentation, and increased patient control over their health information. However, the authors also acknowledge several challenges, such as the need for standardization and the potential for data breaches.

M. A. Alsheikh et al [8], This paper proposes a blockchain-based solution for secure telemedicine and telehealth applications. The authors argue that the current lack of security and privacy in telemedicine systems hinders their widespread adoption. The blockchain-based solution enables secure sharing of patient health information among multiple healthcare providers and institutions, while maintaining patient privacy and confidentiality.

The authors propose a four-layered architecture for the blockchain-based solution, which includes a data layer, identity layer, smart contract layer, and user interface layer. The data layer stores patient health information, while the identity layer ensures secure identification of patients and healthcare providers. The smart contract layer facilitates automated transactions among healthcare providers, while the user interface layer enables patients to access and manage their health information. The proposed solution offers several advantages over traditional telemedicine systems, including improved data security, reduced risk of data breaches, and increased patient control over their health information. However, the authors also acknowledge several challenges, such as the need for standardization and the potential for scalability issues.

M. B. Zaman et al [9], This paper proposes a blockchain-based solution for secure and efficient telemedicine applications. The authors argue that the current lack of security and efficiency in telemedicine systems hinders their widespread adoption. The blockchain-based solution enables secure sharing of patient health information among multiple healthcare providers and institutions, while maintaining patient privacy and confidentiality.

The authors propose a four-layered architecture for the blockchain-based solution, which includes a data layer, identity layer, smart contract layer, and user interface layer. The data layer stores patient health information, while the identity layer ensures secure identification of patients and healthcare providers. The smart contract layer facilitates automated transactions among healthcare providers, while the user interface layer enables patients to access and manage their health information. The proposed solution has several advantages over traditional telemedicine systems, including improved data security, reduced risk of data breaches, and increased patient control over their health information. However, the authors also acknowledge several challenges, such as the need for standardization and the potential for scalability issues.

R. Hassani et al [10], The paper highlights the challenges faced by the industry in terms of data security, privacy, and interoperability and explores how blockchain can address these issues.

The authors emphasize that blockchain can enhance the security of electronic health records by providing a tamper-proof and decentralized system that reduces the risk of data breaches. The use of smart contracts in blockchain can also help to automate healthcare processes such as insurance claims and clinical trials, reducing costs and improving efficiency. The paper also highlights the potential of blockchain in facilitating data sharing between healthcare providers and patients, leading to better-informed decision-making and improved patient outcomes. However, the authors also recognize the challenges that come with implementing blockchain in healthcare. These challenges include regulatory barriers, technical complexities, and interoperability issues. The paper proposes several recommendations for overcoming these challenges, such as creating standards and guidelines for blockchain implementation in healthcare and ensuring that blockchain systems are interoperable with existing healthcare IT infrastructure.

III. EXISTING SYSTEM

Blockchain technology is increasingly being utilized to improve the safety and integrity of the pharmaceutical industry. Several systems have been developed to detect and track pharmaceutical medicine using blockchain. These systems utilize the secure and tamper-proof nature of blockchain to provide a transparent and verifiable record of every transaction in the supply chain.

One such system is MediLedger, which offers end-to-end tracking and traceability of pharmaceutical products. MediLedger ensures the authenticity of drugs and prevents the introduction of counterfeit drugs into the supply chain. The platform utilizes blockchain technology to create a secure and immutable record of transactions, from manufacturer to the patient.

Another system is BlockRx, which tracks the entire lifecycle of a drug, from development to distribution and use. BlockRx incorporates smart contracts to automate the tracking and verification process, ensuring that data is accurate and tamper-proof. This system provides a transparent and secure way to track and verify the authenticity of pharmaceutical products.

FarmaTrust is another example of a blockchain-based platform that aims to prevent the distribution of counterfeit drugs. This platform utilizes a combination of blockchain, AI, and big data analytics to verify the authenticity of pharmaceutical products. By tracking the entire supply chain, FarmaTrust ensures that all drugs are authentic and safe for use.

Lastly, Pharm2Farm provides a secure and tamper-proof supply chain for pharmaceutical products. This system uses blockchain technology to track the entire supply chain, from manufacturer to retailer, ensuring the authenticity and safety of all drugs.

Overall, these systems aim to improve patient safety and prevent the distribution of counterfeit drugs by providing a secure and verifiable record of transactions in the pharmaceutical supply chain. By utilizing blockchain technology, these systems ensure the authenticity and safety of pharmaceutical products.

IV. PROPOSED METHODOLOGY

A. Dataset:

We discovered various datasets that provide us with the minute details regarding several pharmaceutical drugs and medicines. We have learnt above following datasets which govern our problem:

1. **DrugBank:** From [11], A comprehensive database of drugs, drug targets, and drug interactions.
2. **DailyMed:** From [12], A repository of medication package inserts, including information on dosage, administration, and warnings.
3. **U.S. National Library of Medicine DailyMed API**: From [13], Provides access to the same information available on the DailyMed website through an API.
4. **RxNorm**: From [14], A standardized nomenclature for clinical drugs produced by the United States National Library of Medicine.
5. **OpenFDA:** From [15], An initiative by the U.S. Food and Drug Administration that provides access to public data related to drug adverse events, recalls, and labelling.

B. QR Code

A QR code, short for Quick Response code, is a two-dimensional barcode that can be scanned using a smartphone or QR code reader to quickly access information, such as text, URLs, or other data. QR codes are commonly used in various applications, including marketing, inventory management, and authentication.

Blockchain is a decentralized and distributed digital ledger that securely records transactions across multiple nodes in a network. Each transaction is recorded in a block that is linked to the previous block using cryptographic techniques, forming a chain of blocks that is immutable and transparent.

QR codes can be used in conjunction with blockchain technology to create a system for verifying and tracking information related to medicines, such as medicine details, batch numbers, manufacturing dates, and expiration dates. Here's a step-by-step procedure on how QR codes can be used in a blockchain-based system:

Generate QR codes: Medicine details can be encoded into QR codes using a QR code generator tool. The encoded information can include details about the medicine, such as its name, dosage, instructions for use, and any other relevant information.

Attach QR codes to medicine packaging: The generated QR codes can be printed and attached to the medicine packaging, such as the bottle or box, using adhesive labels or other secure methods.

Scan QR codes: End-users, such as patients, pharmacists, or other stakeholders, can scan the QR codes using a smartphone or QR code reader. The QR code scanner can decode the information encoded in the QR code and display it on the screen.

Retrieve information from blockchain: Once the QR code is scanned, the system can access the blockchain to retrieve the corresponding information related to the medicine. The information can be stored in the form of transactions or smart contracts on the blockchain, which can be accessed and verified by authorized parties.

Verify information: The retrieved information can be compared with the information printed on the medicine packaging to verify its authenticity. This can help in preventing counterfeit medicines and ensuring that the medicine is genuine and safe for use.

Update blockchain: As new transactions or changes in medicine information occur, they can be recorded on the blockchain to maintain an updated and transparent record of the medicine's details. This can help in creating a traceable and auditable history of the medicine throughout its lifecycle.

Once you have access to medication information from these or other sources, you can generate QR codes using a free online QR code generator tool. Just enter the information you want to encode in the QR code, such as medication name, dosage, and instructions for use, and the tool will generate a QR code that can be scanned to access this information. Using QR codes in conjunction with blockchain can provide several benefits, such as increased transparency, traceability, and authenticity of medicine information. Additionally, blockchain can provide robust security through cryptographic techniques, preventing unauthorized access and tampering of data. It also eliminates the need for a central authority, making it a decentralized and trust less system.

It's important to note that proper data privacy and security measures should be implemented to protect sensitive information, such as patient data, in compliance with applicable regulations and laws. Additionally, the implementation of a blockchain-based system with QR codes for medicines would require careful consideration of technical feasibility, scalability, and usability aspects, as well as compliance with relevant industry standards and guidelines.

D. Blockchain Techniques:

The blockchain technology primarily focusses to maintain privacy of the model proposed in the study and involves various techniques to prevent the loss of information or confidential data during transactions. This paper would discuss the following techniques in blockchain domain:

1. **Public Blockchain:**

In the case of [16], a pharmacy fraud detection and security system that utilizes a public blockchain, the system can be built using a decentralized and public blockchain network like Bitcoin or Ethereum. Smart contracts can be utilized to define the rules and logic for the fraud detection and security process. The system can use QR codes as a means of input to trigger smart contracts that perform the necessary checks and verifications to ensure the authenticity of the pharmaceutical product. Since a public blockchain is a decentralized network, it provides a high level of transparency and accountability, as all transactions and data are visible to all participants. Therefore, it can be easier to track the history of a drug from the manufacturer to the pharmacy, and to identify any potential fraud or tampering in the supply chain.

However, using a public blockchain may also have some disadvantages, including scalability issues and high transaction fees, as well as the possibility of a 51% attack, where a single participant or group of participants control more than half of the network's computing power.

2. **Consortium Blockchain:**

In [17], A consortium blockchain approach involves building a shared blockchain network between a group of pharmacies to collaborate on fraud detection and security. In this approach, the pharmacies can create a private and permissioned blockchain network that is only accessible to authorized participants. Each participant will have a node in the network and can contribute to maintaining the blockchain.

QR codes can be used to facilitate secure transactions and data sharing between the pharmacies. When a QR code is scanned, it can trigger smart contracts that perform necessary checks to verify the authenticity of the pharmaceutical product. By collaborating on a shared blockchain network, the pharmacies can reduce the risk of fraud and increase the security of the supply chain.

Since a consortium blockchain is a permissioned network, it provides greater control and privacy than a public blockchain. The network can be designed to meet the specific needs of the participating pharmacies, and transactions can be processed quickly and efficiently with lower transaction fees.

However, the consortium blockchain approach may have some limitations, including the need for a trusted network administrator to manage and maintain the network, as well as the potential for data silos between participating pharmacies.

3. Hybrid Blockchain:

A hybrid blockchain approach combines the benefits of both public and consortium blockchains. In this approach, a public blockchain can be used for auditing and transparency purposes, while a consortium blockchain can be used to facilitate secure data sharing between the pharmacies.

QR codes can be used to trigger smart contracts that implement the fraud detection and security process. The public blockchain can be used to record and verify transactions and provide transparency and accountability to the system. The consortium blockchain can be used to facilitate secure data sharing and provide greater control and privacy to the participating pharmacies.

The hybrid blockchain approach offers greater flexibility and scalability than the other two methodologies. The participating pharmacies can choose which transactions to record on the public blockchain and which ones to keep private on the consortium blockchain. This approach can provide a balance between transparency and privacy, while also improving the efficiency and security of the system. However, it may require more complex infrastructure and management compared to the other two approaches.

E. Model Architecture:

Model selection and implementation are important steps in the deployment of our model. The study would introduce the architecture of the model with a simple flowchart represented as:

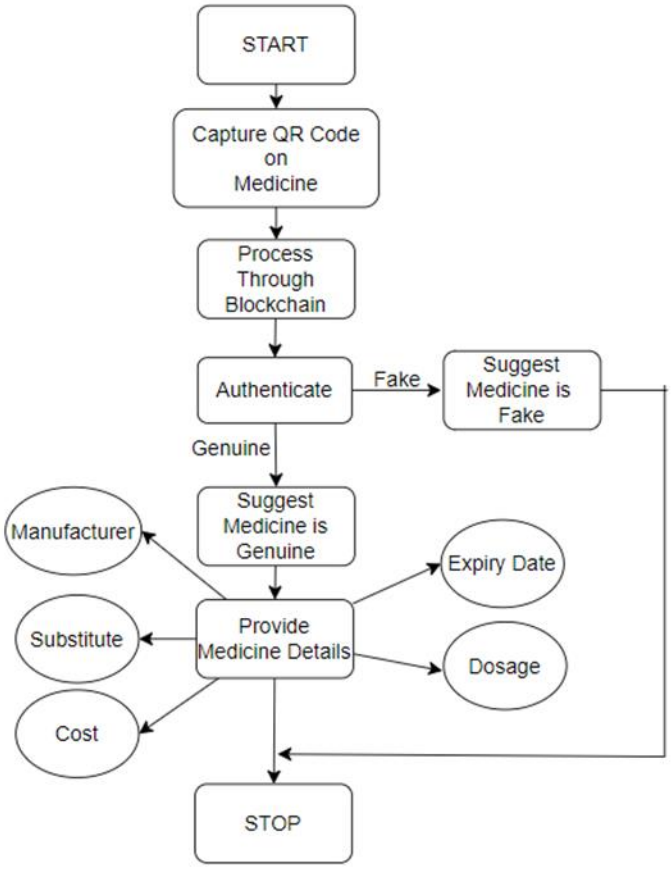

Figure-1: Model Flowchart

The model would Involve various steps from capturing the QR code on medicine or User provided input and process it through a secure Blockchain based environment to maintain privacy and preserve information.

V. COMPARATIVE ANALYSIS

In this study, we evaluate our model against already existing systems along with the appropriate technique and execution. The model's performance is then compared with other models, such as traditional methods or other medicine prescribing system, on the similar dataset or metrics. This step allows for a comprehensive evaluation of the model's performance and to identify its strengths and weaknesses. Also, our model is a QR code-based model which makes use of Blockchain to preserve information and ensure privacy. Thus, being superior to some of existing systems due to an improved and a secure option.

VI. RESULT AND CONCLUSION

Based on the various types of blockchain based systems used for medicine or drug recommendation we foreshadowed the multiple types of technologies used and found out that the consortium blockchain is highly recommended. A Consortium Blockchain is privately owned but not only by a single entity or company. A blockchain is instead owned by an association of individuals from various industries or a group of organisations. It also differs in function since a consortium blockchain is used to coordinate data from different sources, thus promoting collaboration and upholds variety of data. This would be the fundamental block of the model proposed

In this study as it is a robust, scalable and most important reliable for maintaining privacy for various users and transactions.

REFERENCES

1. "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy" by S. S. Hussain, S. Tahir, A. Almogren, and A. Albeshri
2. "Blockchain-Based Secure Framework for Healthcare Applications" by J. Choi, J. Chung, and S. Kim
3. "Blockchain-Based Decentralized Control for Healthcare Systems" by S. S. Hussain, S. Tahir, and M. A. Alam
4. "A Blockchain-Based Framework for Secure and Privacy-Preserving Healthcare Information System" by Y. Zhang, X. Xu, Y. Ren, and H. Guo
5. "A Blockchain-Based Approach to Enhancing the Security and Privacy of Electronic Health Records" by A. V. D. Perera, D. N. Ranasinghe, and X. Li
6. "A Blockchain-Based Electronic Health Record System for Healthcare Services" by S. S. Lee, S. Kim, and K. Kim
7. "Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability" by J. M. Ahram and E. O. H. El-Masri
8. "Blockchain Technology for Secure Telemedicine and Telehealth Applications" by M. A. Alsheikh, F. A. Tawalbeh, and M. Al-Qutayri
9. "Secure and Efficient Blockchain-Based Approach for Telemedicine Applications" by M. B. Zaman, M. A. Uddin, and M. S. Islam
10. “Blockchain in Healthcare: Opportunities, Challenges, and Recommendations" by R. Hassani and S. K. L. Kiah
11. Wishart, D. S., Feunang, Y. D., Guo, A. C., Lo, E. J., Marcu, A., Grant, J. R., ... & Djoumbou Feunang, Y. (2018). DrugBank 5.0: a major update to the DrugBank database for 2018. Nucleic acids research, 46(D1), D1074-D1082. doi: 10.1093/nar/gkx1037
12. U.S. National Library of Medicine. (n.d.). DailyMed. Retrieved April 23, 2023, from https://dailymed.nlm.nih.gov/dailymed/
13. U.S. National Library of Medicine DailyMed API: U.S. National Library of Medicine. (n.d.). DailyMed API. Retrieved April 23, 2023, from https://dailymed.nlm.nih.gov/dailymed/webservices-help/v2/DrugAPI.htm
14. Liu, J., Zhao, S., Zhang, Y., & Zhao, Y. (2016). RxNorm: An overview of clinical drug information. Expert review of clinical pharmacology, 9(1), 81-89. doi: 10.1586/17512433.2016.1128703
15. U.S. Food and Drug Administration. (n.d.). OpenFDA. Retrieved April 23, 2023, from https://open.fda.gov/
16. M. Stojanović, D. Stanković, and Z. Djurić, "A blockchain-based approach for drug supply chain traceability and fraud detection," Journal of Medical Systems, vol. 43, no. 8, Aug. 2019.
17. N. Suryadevara and S. Krishnan, "A blockchain-based secure and scalable system for healthcare data sharing," Journal of Medical Systems, vol. 42, no. 8, Jul. 2018.
18. R. S. Bahga and V. K. Madisetti, "HybridBlock: A hybrid approach to blockchain-based security for healthcare," Blockchain in Healthcare Today, vol. 1, Nov. 2018.