FAKE DRUG DETECTION USING QR CODES AND CONSENSUS BASED SECURITY ENHANCEMENT IN DECENTRALIZED BLOCKCHAIN SYSTEM

GADDE PRANITHA[1] AND P.V.LAKSHMI[2]

[1] Research Scholar, Computer Science Engineering, Gitam University,
Visakhapatnam, Andhra Pradesh, India
[2] Professor, Computer Science Engineering, Gitam University,
Visakhapatnam, Andhra Pradesh, India
E-mail: pranitha513@gmail.com, pvl.7097@gmail.com

ABSTRACT

Fake medicines are becoming a growing problem in the pharmaceutical industry's field of piracy and manufacturing. Implementing QR codes in the manufacturing process is one way to address the problem of fake medication. But however, it cannot solve the problem completely and so that the novel Decentralized blockchain assisted Quick response (QR) code system (DcB assist QR) is introduced in this research work. In this work, once if the drugs are created by the manufacturer, the QR is generated for the corresponding drugs. After that particulars are uploaded in the blockchain once gotten approval of government, then it can be distributed over the hospitals. The drug details are stored securely into the blockchain, so that intruders are cannot accessed and modify the drug details. In blockchain, the data are encrypted using hyper elliptic curve based cryptosystem (HEllC) model. Further, to secure the blockchain network and prevents unauthorized users from validating bad transactions, an Improved Practical Byzantine Fault Tolerance (IPBFT) consensus algorithm is proposed for effective block verification. During drug transportation, the temperature monitoring of drugs is enabled by Internet of Things (IoT) sensors and whenever temperature crosses the threshold, the alert message is send to the driver of the vehicle. Especially, an Inter Planetary File System (IPFS) is employed to store drug temperature data in a decentralized way. Moreover, the performance of the DcB assist QR system evaluated based on various several performance metrics and compared to existing system. The DcB assist QR system attained 21.02 seconds of less execution time and 983.7 kBps of throughput.

Keywords: *Blockchain, Hyper elliptic curve, Improved Practical Byzantine Fault Tolerance, Inter Planetary File System, Fake Drug detection, QR code, Encryption.*

1. INTRODUCTION

In this technological era, Counterfeit Pharmaceutical Prevention plays a vital role to analyse the drug is real or fake. The fake drug have various ingredients than original drug known as counterfeit drugs used to cure the disease, but it harmful to health. Some of the fake drugs have wrong active ingredient, no active ingredient and incorrect quantity of right ingredient [1]. Sometimes the substandard drug have dangerous ingredient which affect patient's health and causes mass poisoning. WHO said "A product that is purposefully and illegally mislabelled with regard to its origin or identity". It's a critical problem to counterfeiting drugs which affects public health and loss of revenue for government [2]. Several techniques were already developed to identify and trace the counter drugs in medicine supply chain. There are several tracking methods used to trace the drugs which is highly injurious [3].

Generally, the Data-Matrix tracking system was widely used to detect the fake drug. It contains unique ID, Manufacturer ID, Product ID, optimal meta-data and authentication code used to recognize the fake drugs [4]. Sometimes, counterfeiting the drug manufactured and modified with some popular or reputed pharma company logo to sell on market without any hurdles [5]. Few popular and expensive medicine such as painkiller, cardiac medicines cancer, antibiotics were counterfeited to sell in market using their identity. Nearly, 10 to 15% of drug are fake and are majorly manufactured in developing countries [6]. Around 30% of drugs are manufactured over a year and 0.2 millions of people became dead due to this counterfeit drugs. In this 21st century, counterfeiting drug is one of the rapidly growing business reported by International Anti-counterfeiting coalition (IACC) [7, 8]. Due to increasing cause of several diseases and urge to cure the disease, several number of drugs were introduced in the market using the fame of popular brand medicine [9].

According to estimates, the global market for drug sector will be worth US$1.2 trillion in 2021 rather than US$930 billion in 2018. Analysing the quality and quantity of drug is essential for drug manufacturing, developing, marketing and patient use [10]. Some of the drug analysis techniques were used to detect the quality of drug named as gas chromatography (GC), mass spectrometry (MS), high-performance liquid chromatography (HPLC) and capillary electrophoresis (CE). But, these techniques were expensive and requires highly trained operator, extensive sample preparation and equipment [11, 12]. Radio Frequency identification (RFID) code are used for data-matric tracking to identify the drug is fake or real. Several researchers' approach RFID for data-matric tracking but, it is expensive for implementation based on medicine price [13]. Hence, the QR code is a new authenticity technique to verify the drug as original or fake by scanning. Simply, the QR is widely used to verify the authenticity of every physical product [14, 15].

The QR code labelled on drug includes the sensitive information like chemicals or ingredient used in drug, batch number, manufacturing and expired date of drug using online digital verification check [16]. Cryptography is a quite popular technique to provide a secure communication using encryption and decryption. When sensitive data are required to be secure and prevent the data from third party, block chain technology is widely used [17]. Using the cryptography technique, only authenticated person can access the data. Blockchain is widespread technology majorly used to store the data with high security [18]. On considering the real-time challenges and opportunities of blockchain-powered healthcare systems, creating an opportunity to identify gaps to come up with a unique solution is required [19, 20].

1.1 Motivation

Counterfeit drug detection is an essential technique to identify the quality of drugs. Several techniques and tests were used to detect the quality of the drug. But it is a long process and takes more time to identify whether the drug is original or fake. So, a QR code is used to identify the drug, which contains every piece of information about the drug, such as batch number, ingredients used in the drug, manufactured date, and expired date. This approach can provide better security for this drug information when stored on blockchain. Some of drawbacks obtained in fake drug detection by only QR code scanning are increased risk of data loss, less accurate in some cases and so on. Some techniques are difficult to address the attacks over the information of drug. Also, because of limited resource of drug details, it becomes complex to detect fake drugs. It is highly critical to manage the pharmaceutical supply chain during data transactions whereas a clear vision of drug information and identification cannot be obtained. In most of the existing works, less security is provided over third-party access and may result in ransom or DoS attacks. Because of inappropriate handling of data, less transaction speed and lower throughput are resulted. These issues motivated to propose a novel technique for counterfeit drug detection based on QR code assisted block chain with encryption methods to enhance the model efficiency. The major contributions of the proposed work are given as below.

- To present a decentralized blockchain system assisted QR code for promoting better authentication in preventing the intrusion of fake drugs.
- To encrypt the transaction data to be stored in the block chain using Hyper-elliptic curve based cryptosystem (HEllC) model.
- To secure the blockchain network from unauthorized users, Improved Practical Byzantine Fault Tolerance (IPBFT) consensus algorithm is employed.
- To store the sensor related information of drugs in Inter Planetary File System (IPFS) for maintaining the efficiency of blockchain.

The research paper is organized as four different sections. In section 2, several existing research works based on the fake drug detection are described. In section 3, the proposed methods for improving the security to the medicine details in the blockchain are explained. In section 4, the DcB assist QR system is evaluated based on several performance metrics and its results are discussed. In section 5, conclusion, future work and references are given.

2. RELATED WORKS

Some of the related works over fake drug detection using blockchain are surveyed and described as follows.

Saroj Kumar Nanda, et al. [21] introduced a novel approach for integrated Internet of Things

(IoT) with blockchain in Health Supply Chain (NAIBHSC) approach. It used to eliminate every chain-related problems and combine the blockchain technology with IoT developed smart health supply chain management system. It provide trust, security, visibility, privacy, avoid counterfeit drugs, cost reduction, and avoid damaged medical components, authentication, decentralized tracing and tracking of drugs. Smart contracts were developed by solidity programming language with public permission Ethereum blockchain technology. It reduce latency time, improve response time and performance. The performance of this model does not provide feasibility in real-time environment.

Mueen Uddin, [22] proposed novel track and trace blockchain-enabled Medledger system that leverage Hyperledger Fabric blockchain platform using chain codes. This model used to securely process the drug supply chain transaction efficiently through fabric enabled private permissioned distributed network. This model provide authority, safety with high integrity, reliability, security and reduce the likelihood of meddling. Chain codes were designed to control interaction with the stakeholders and drug supply chain ecosystem. It store the records about transaction and events in block chain's immutable Medledger with peer-to-peer decentralized file system named IPFS, file coin, Swarm and so on. It can't provide solution or address critical challenges.

Ethereum blockchain-based approach presented by Ahmad Musamih, et al. [23] which leverages smart contract and decentralized off-chain storage in healthcare supply chain for efficient product traceability. This model provide secured immutable history over the transaction of stakeholders and eliminate needs for intermediaries. This model secure the data from malicious attempts targeting is integrity, non-repudiation of transaction and availability which is complex and critical for pharmaceutical supply chain.

Ghaith Khalil, [24] proposed an RFID-based anti-counterfeiting and anti-theft scheme used to identify the counterfeit drug at point of purchasing. This model use low-cost passive tags for suited and lightweight organisation of large scale retail environment. Tran and Hongs anti-counterfeiting protocol were analysed and used to address of some limitation. This model provide security which satisfy authentication . Some of resistant were occurred to security attacks named DoS attacks and database spoiling. Track and trace technique over RFID based anti-counterfeiting use medium resource and increase risk of data loss.

Herbert Melendra Garcia, et al [25] proposed drug query system which provide reliable data on origin and authenticity of product. Security preservation and integrity of exposed information were stored using Blockchain technology. The information such as characteristic details of drug, active ingredients, pharmaceutical form and composition were briefly described in blockchain. This model was aimed to identify the commercial origin of drug and evaluate the qualitative and quantitative detail of drugs. Limited resources were acceptable for transaction. The surveyed techniques over fake drug detection using blockchain is analysed in Table 1.

Table 1: Survey Of Existing Works With Its Performance And Limitation

Author name and year	**Techniques used**	**Limitation**	**Performance**
Saroj Kumar Nanda, et al. 2023	NAIBHSC approach	This model does not provide feasibility in case of real-time environment.	Response time, latency time
Mueen Uddin, 2021	Novel track and trace blockchain-enabled Medledger system	It can't provide a better solution or address critical challenges of security.	Scalability limitations, costs of operating, data privacy
Ahmad Musamih, et al. 2021	Ethereum blockchain-based approach	It is highly complex and critical for pharmaceutical supply chain management.	Cost analysis and security analysis
Ghaith Khalil, 2020	RFID-based anti-counterfeiting and anti-theft scheme	It increases the risk of data loss and effective security cannot be obtained.	Nonce test, RFID tag counterfeit, computation and efficiency.
Herbert Melendra Garcia, et al. 2020	Drug query system using blockchain	Only Limited resources can be acceptable during data transaction.	Variation of transaction and throughput.

Fake drug detection is the important process in the medical field as it had created the major issues for the patient health. But not effective medical supply chain and medicine details are stored and accessed in the medical fields. That created caused the growing amount of fake drug, which not approved by the government. So that novel methodology developed for securely store the data into the blockchain.

3. PROPOSED METHODOLOGY

The medical trade faces a serious issue with fake medicines, especially in countries that are developing where regulatory control can become laxer. The goal of the proposed work is to provide a blockchain-based solution for the growing problem of fake medications in the pharmaceutical sector. The proposed blockchain based work securely store and track the medicine details. Proposed work architecture is represented in Figure 1.

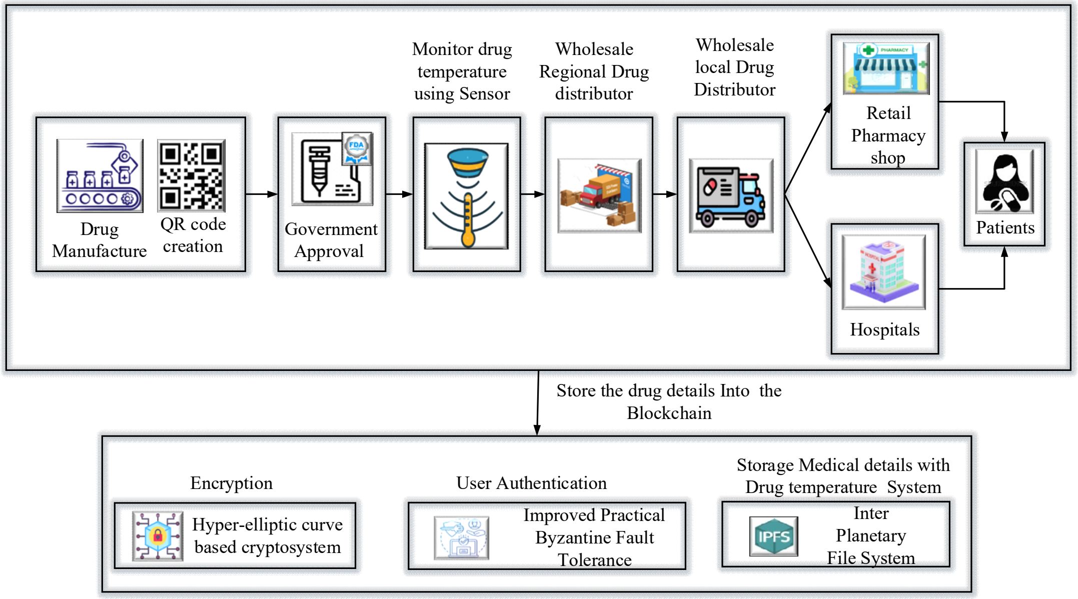
Monitor drug temperature using Sensor
Wholesale Regional Drug distributor
Wholesale local Drug Distributor
Retail Pharmacy shop
Drug Manufacture
QR code creation
Government Approval
Patients
Hospitals
Store the drug details Into the Blockchain
Encryption
User Authentication
Storage Medical details with Drug temperature System
Hyper-elliptic curve based cryptosystem
Improved Practical Byzantine Fault Tolerance
IPFS
Inter Planetary File System

Figure 1: Structure of the DcB assist QR system

In this fake drug detection system, the initially, QR code is generated for the every medicine after the manufacturing is completed. Then after the medical details are send to the government for get approval. After getting the approval the medical details are stored into blockchain for access data and tracking the drug transaction without any modification of the drug during the transaction. Additionally, the temperature details of the drug also updated eventually by using the IoT sensor node. That also will be helpful to know any fake included into the transaction. Using the HEllC encryption techniques, the drug details are securely transacted over the network. IPBFT techniques effectively authenticate the user and finally the IPFS file storage used for the storing the drug details with high security. The details explanation of the secure blockchain mechanism is provided into the following sub-section.

3.1 Data Encryption Using Hyper-Elliptic Curve Based Cryptosystem

Hyperelliptic curve is a modified version of elliptic curve and it is a type of algebraic curve. Nevertheless, HEC points have not been collected from the group. The modified Abelian group has been gathered using the divisor or else HEC computation. The integration of elliptic curve, RSA and bilinear with HEC provide some advantages such as it produced the similar security by utilizing a less parameter size. The elliptic curve represented with the values of genus 1. In a similar manner, the ensemble structure of the finite field (ff) for the (genus $V = 1$) required 160-bit wide operands that requires at least $k.\log_2(w) = 2^{160}$. Similar like this, curves having genus 2 which needed operands that are 80 bits length while curves with genus 3 which is demand operands that are 54 bits length. A group of solutions to the equation $(p,q) \in T \times T$ comprises a hyper elliptic curve L with genus $k(k > 1)$ across T .

$$L : q^2 + n(p)q = t(p) \qquad (1)$$

Where, HEC divisor is represented as V that is a certain amount of points, which is expressed as below.

$$V = \sum_{u_l \in L} o_l u_l,\; o_l \in X \qquad (2)$$

Two assumptions of complexity is taken into the consideration such as Hypothesis of Hyperelliptic Curve Discrete Logarithm Problem (HECDLP) assume the following ideas for HECDLP. β be the member of $\{1,2,3,\ldots\ldots,w-1\}$ and However, there is a small probability (β) estimated using $I = \beta \times V$. β and α are the member of $\{1,2,3,\ldots\ldots,w-1\}$ and the computation probability of β and α using the $\Gamma = \beta \times \alpha \times V$, which is small in algorithmic Hyperelliptic Curve Diffie-Hellman Assumption (HECDHA). The both encryption and decryption procedures used publicly identified HEC parameters that comprises the $L(ff)$ that is defines as HEC on a finite field (ff), large prime number (Pim). Both sides even more accept of additional parameters $\{w, ff, L(ff), V, e\}$ as well as to these basic parameters. The symbol for the encrypted message is O_Msg . The two groups are share a common key such as $K_y = (rs)V \;\; Jn(ff)$ after the encryption and decryption decided with the parameters, which is the diminished the divisor of the Jacobian. The first party encrypting the message O_Msg via this key and generating the ciphertext C_T , after that sends it to the other party. The other party obtains the ciphertext C_T and decrypts it with the shared key, after that it recovers the original message through the following algorithm. Table 2 contained the algorithm for HEC based encryption in the sender side and Table 3 contained the algorithm for HEC based decryption in the receiver side.

Table 2: Encryption Based On HEC

Algorithm 1
Input: Original message O_Msg , Receiver's public key (Pu_K_R) and domain parameters.
Select a random number $r \in [1, w-1]$ Compute $r.Pu\_K_R$ Return the cipher text using $C\_T = O\_Msg + r.Pu\_K_R$
Output: Cipher text C_T

Table 3: Decryption Based On HEC

Algorithm 2
Input: Cipher text C_T , Sender's public key (Pu_K_S) , domain parameters and Receiver Private Key (Pa_K_R)
Compute $Pu\_K_R \times Pa\_K_R$ Return original message as $O\_Msg = C\_T - (Pu\_K_R \times Pa\_K_R)$
Output: Original message O_Msg

HEC-DH time complexity is generated using the following equation.

$$Time_{HEC-DH}(o) = R_t 2^2 (2o^2 - 1) = a(2^{o^2}) \qquad (3)$$

Where, R_t is represented the time required for several addition operation and o denoted as the exchanged public key among the receiver and sender. After finishing the encryption process of the all medicine details, the confidential medicine details are stored into the blockchain. If anyone need to access the medicine data they only receive encrypted data. The receiver need to decrypt it using the sender public key and its private key.

3.2 Authenticate User Using Improved Practical Byzantine Fault Tolerance

If someone need to access medicine data, the user must be authenticate by some secure mechanism. So that, the proposed work utilized IPBFT. Blockchain is attracting an extensive amount of media attention to be a typical Peer-to-Peer (P2P) network architecture application because of its decentralization and confidentiality characteristics. However, as a result of its fundamental characteristics, malicious nodes can attack blockchain. Throughout the field of consensus, limiting the influence of malicious or misleading nodes inside the system. The consensus techniques IPBFT consists of three phases as Evaluation of node trust, generating the consensus group and consensus procedure. IPBFS structure is given in Figure 2.

IPBFS will initially propose the Eigen-Trust model, in order to determine the global trust value for each node that will serve as the foundation for choosing the consensus group. After that, the greatest trust value contained nodes is chosen onto the consensus group. A large-scale networked system can benefit from a more efficient consensus process because a smaller number of nodes would participate in it due to the inclusion of a consensus group. Then, another block can joint to the blockchain and latest transaction among the nodes. So that, global trust value may automatically modified within a block and the next phase is permitted through the IPBFT.

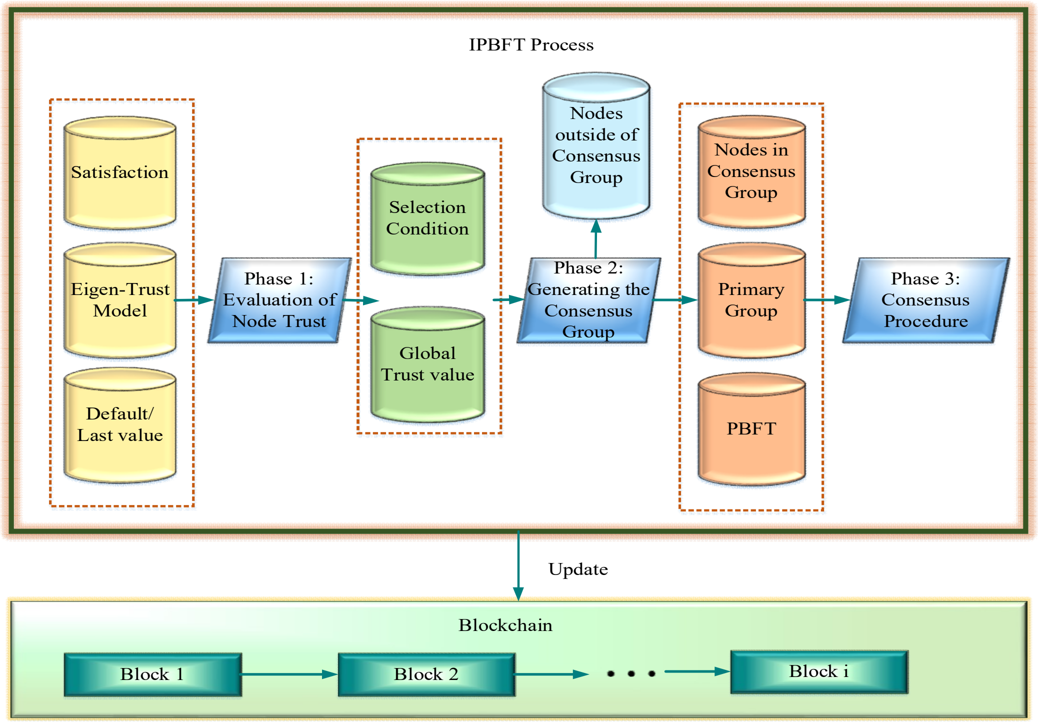

Figure 2: IPBFS structure

3.2.1 Evaluation of Node trust

In this stage, it shows the evaluation of trust node procedure by using the Eigen-Trust method. The system support C number of nodes within the network, assigned the global trust value for each node to $^{1}/_{C}$ in the system and calculated the direct trust value among nodes through directly trading. Calculate an appropriate trust value for nodes which cannot communicate with one another directly. In the end, these can be employed to calculate the global trust value.

Divide Node algorithm classifies the every nodes consider transmission relationship among the nodes for calculating the recommended trust value and direct trust value. If a particular $node_k$ makes a transaction with another node, that node is placed into the group known as TN node group. If not, it is placed into the $NonTN$ node set. Table 3 contained the algorithm for Node division.

Table 4: Algorithm For Node Division

```
Algorithm 3
Input: $N_k$, node set- $N$
$TN \leftarrow \Phi, NonTN \leftarrow \Phi$
for $N_k \in N$
    if $N_k trades\ with\ N_k$
        $TN \leftarrow N_k$
    else
        $NonTN \leftarrow N_k$
    end
end
Output: $TN$ or else $NonTN$
```

Here, TN and $NonTN$ referred as the Tx-node and NonTx-node, $K-th$ node denoted as N_k and N represented the node. The algorithm 4 and 5 are the direct trust value and recommended trust value computation process respectively. Table 4 shows the algorithm for calculating the trust value for the TN nodes. As illustrated via Algorithm 2, after receiving the inputs N_k and its direct transaction collection TN the method searches the historical records containing satisfied and dissatisfied interactions to calculate the absolute satisfaction score D_{kl}. Table 4 contained the Node Trust calculation for Tx-node

Table 5: Algorithm For Calculating The Node Trust For Tx-Node

```
Algorithm 4
Input: $N_k$, $TN\ of\ N_k$
---
$D_{kl} \leftarrow 0$
for $N_k \in TN$
    $H_{kl} = sat(k,l) - un\_sat(k,l)$
  end
if $H_{total} = 0$
    $D_{kl} = \frac{1}{C}$
else
    for $N_k \in TN$
        $D_{kl} = \frac{\max(H_{kl},0)}{H_{total}}$
  end
end
---
Output: Direct trust value ( $D_{kl}$ )
```

The recommended trust computation process used the N_k, all nodes presented in the $NonTN$ which aren't carry out the transaction by using the N_k as the output. Identifying the transaction routes and generating the by manipulating these direct trust values is the fundamental approach in this system. The N_k must obtain $N_k \in NonTN$ that have completed transactions to the target N_l for calculating the recommended trust value for N_l that have not performed any transactions with N_k. Through the outcome of the D_{km} and D_{lm}, recommendation trust value among the N_k and N_l is calculated. In the case of no one perform, calculation of the recommended trust value is done by applying the various transaction routes repeatedly. Table 5 shows the algorithm for calculating the trust value for the $NonTN$ nodes.

Table 6: Algorithm For Calculating The Node Trust For Nontx-Node

```
Algorithm 5
Input: $N_k$, $NonTN\ of\ N_k$
---
$D_{kl} \leftarrow 0$
Identify the transaction path among the $N_k$ and $N_l$.
for $N_k \in NonTN$
  if $N_k \in TN\ of\ N_k$ & $N_k \in TN\ of\ N_l$
    $D_{kl} = \sum_m D_{km} D_{lm}$
  else
      Iteratively calculate the $D_{kl}$.
  end
end
---
Output: Recommended trust value ( $D_{kl}$ )
```

All nodes then form a local trust relationship and displays a local trust value with high accuracy. Also need to calculate the global trust value in order to get the trust value that accurately represents the node's level of trust. Table 6 shows the algorithm for calculating the Global trust.

Table 7: Algorithm For Calculating The Global Trust.

```
Algorithm 6
Input: $N_k$, node set- $N$
---
$G_k \leftarrow 0$
for $N_l \in N$
    $G_k = \sum_m G_l D_{lk}$
end
---
Output: Global trust value ( $G_k$ )
```

In the first phase, all nodes have a value of 1/N, where N is the total number of nodes in the system. The node must recalculate its global trust value each time a new block is created. The global trust value of N_k must be equal to the combined amount of its local trust value and an equivalent global trust value for the other node. Every other node in the network possesses an impact on the dynamic global trust value. It may help in reducing certain low credit nodes achieving consensus by obtaining accurate node trusts via the application of this comprehensive dynamic evaluation mechanism.

3.2.2 Generating the consensus group

In this stage, the details of blockchain consensus group creation process is described. The Eigen Trust model estimates the global trust values of each node in the system. Consider that nodes with greater global trust values are viewed as more trustworthy when evaluating personal profit driven variables, based on the assumption of behavior reliability. By selecting a subset of the blockchain consortium nodes with greater trust levels rather than all of them, it is possible to increase the efficiency and scalability of blockchain consortium consensus procedures. The Byzantine fault-tolerant rate can be increase by removing the less credit nodes. Conversely, by limiting the ability of blockchain consensus nodes, it may speed up the delivery of messages and enhance the consistency of the blockchain consensus process.

A node that achieves the specified trust threshold in terms of global trust value has been chosen to compose the blockchain consensus group. Nevertheless, this would produce an extensive variation with the number of blockchain consensus nodes, which would not be helpful to the reliability of blockchain consensus consistency, because the global trust values of nodes are dynamic within a finite amount of time. As a result, it uses a different approach to create the consensus group. The approaches identify a certain percentage of nodes with higher global trust scores. Table 7 represented the algorithm for generating consensus group.

Table 8: Algorithm For Get Consensusgroup

```
Algorithm 7
Input: $N -$ node set, $G -$ Global trust, $p -$ constant percentage of nodes ($0 < p \leq 1$)

$Consensus\quad Group \leftarrow \Phi$
Sorting the $N$ through the Global trust.
for $N_k \in N$
    if $G_k$ is presented in the top of $p$
        Include the $N_k$ in ConsensusGroup
    else
        Remove $N_k$ from the ConsensusGroup
    end
end
Output: Consensus Group
```

Algorithm 7 sorts all of the nodes according to their global trust values after initially setting up a null ConsensusGroup. The process will add N_k to ConsensusGroup if the given a constant proportion of nodes p and a node in the N group Nodes and its global trust is among the top p. Otherwise it neglected from the ConsensusGroup. At the end of the process, from the $N -$ node set the p percentage of nodes are select with the large global trust value for generating the ConsensusGroup in blockchain. The next consensus process in the blockchain only permitted the node which is members of the ConsensusGroup. By executing this, it could significantly improve the blockchain consensus process by choosing the subset of consortium blockchain nodes with the greater global trust values. It is best to avoid modifying viewpoint as much as possible because it is costly and complicated.

3.2.3 Consensus procedure

In this stage, by using the IPBFT consensus algorithm based on the blockchain techniques increase the fault-tolerate rate. After that the ConsensusGroup is generating, the novel block can be created through the participation inside the ConsensusGroup. When the initial node in PBFT fails due to a network outage or a Byzantine node performing erratically, the replica nodes which durations have run out will recognize the issue and initiate a view change process. To reduce the possibility of a view modification procedure and sustain the primary node's Byzantine behavior as well as fail-stop fault, the procedure subsequently chooses a small number of ConsensusGroup nodes with greater trust levels to create the primary group, which will eventually substitute for the primary node. Table 8 described the algorithm for getting primary group.

Table 9: Algorithm for Get Primarygroup

```
Algorithm 8
Input: ConsensusGroup, $f$ – fixed proportion ( $0 < f \leq 1$ )
$primary\ \ Group \leftarrow \Phi$
for $N_k \in$ Consensus Group
    if $N_k$ into the top $f$ with the global trust value.
        Insert $N_k$ in PrimaryGroup.
    else
        Drop $N_k$ outside the PrimaryGroup.
    end
end
Output: PrimaryGroup
```

Primary group's selection procedure is determined by the node's global trust value. The main group is in responsibility for creating, documenting, and verifying the accuracy of the newly generated block. The primary group concept can decrease the difficulty of the view modification task created by the Byzantine behavior or one primary node failure. The IPBFT process has been splitted into the four different steps such as group process, reply, prepare and pre-prepare.

Step 1: Group Process stage

In this stage, Transactions will be packaged by a primary group node into a pre-generated block and propagated to member of the other primary group nodes enabling cross-group monitoring and validation. After authorization, the pre-generated block is going to be temporarily recorded with the same view on each primary group member node. Even though a node within the primary group failures, it can be changed over immediately and fails to initiate the view change process.

Step 2: Pre-prepare stage

In order to facilitate monitoring and verification, the primary group will broadcast a pre-prepare message to each of the replica nodes within the consensus group that containing the pre-generated block as well as the group signature. The group signatures are used to improve the privacy of the main group member nodes and decrease the probability of attacks, and this additionally lowers the possibility of view changes. In other words, any node can confirm the validity of the primary group signature, although it is unable to identify the primary group member.

Step 3: Prepare stage

The replica nodes will independently verify the pre-generated block's validity during the prepare phase. Every duplicate node would compute the block hash after generating the operation of the packed transactions in the pre-generated block with the predetermined transaction sequence. The validity verification succeeded when the result matched the block hash as of the present moment. After the verification, it will send the prepare message also includes the corresponding signature to all other node. After receiving the number of prepare message through the consensus nodes that greater than $2s$ and it pass the reply message to the client, here s is the amount of Byzantine nodes across the consensus group.

Step 4: Reply stage

In the reply stage, the pre-created block is permitted and it will include into the last node of the blockchain while the $s+1$ similar reply message received by client end. Thereafter, each node within the blockchain network will modify its local records.

IPBFT obviously promotes PBFT operation significantly easier through reducing the possibility of a view change among the primary group. In addition, the primary group's member nodes will dynamically migrate in order to generate valid blocks during the consensus process. This is caused by the reason of the any additional transactions will be confirmed after the creation of a new block that leads for altering the overall trust value across all nodes.

3.3 Store The Drug Details In Inter Planetary File System

IPFS is the decentralized storage mechanism for storing the confidential file into the blockchain. Content-addressing was utilized in the creation of IPFS for finding files in a global directory that joins all of the network's generate nodes. Utilizing fundamental file storage infrastructure and without centralized server, the IPFS functions provides a networking protocol inside peer-to-peer systems enabling data retrieval, delivery and storage. According to BitTorrent, all nodes involved in the network can upload new content or receive previously stored content from distributed storage. During discovery and recovery tasks, when a file is located in the decentralized storage that the distributed hash table (DHT) utilized for enables content-addressing.

IPFS is a highly secure system with outstanding performance, data addressability, block storage that supports huge quantities of data storage, and broad simultaneous user access. Every document uploaded into the system via IPFS generates an individual hash address which enables it to receive the content addressed. The same hash address is returned every time an identical data file gets uploaded into the system, even if it has been submitted multiple times. The system can maintain regularity because every node's file has an identical hash address. When the IPFS system is used in blockchain design, it reduces the need for complete nodes while maintaining network transparency. The IPFS file storage acceptable any type of digital transaction, so that it implemented in vast amount of application.

The IPFS de-duplication technique is solved the problem of data redundancy in decentralized networks. Through using the combination of de-duplication and decentralization techniques, the system can become more effectively remove the unwanted storage space. For any new network nodes or nodes rejoining the network after a break, coordination is easier and more rapid because blockchain network nodes only have addresses of data in their transactions instead of a significant amount of data itself. IPFS integration for offline storage solves the primary scalability difficulties in blockchain networks, which is related to storage problems. Additionally, data is permanently saved in the IPFS network, making it secure and robust against hacking. IPFS has four primary building blocks in its architecture to achieve low cost, high throughput, high performance and security. The four primary building blocks of IPFS are Self-Certifying File Systems (SFS), BitSwap protocol, Distributed Hash Table (DHT), and Merkle Directed Acyclic Graph (DAG) structure.

3.3.1 Distributed hash tables

In a decentralized network, key-value pair storage is provided via DHTs. The value of data uploaded to the IPFS network is its data, and the key is the corresponding hashes. Whereas the entire table being replicated across all nodes in the distributed network, each node has a section of the DHT database. A peer gets a request for the key's associated value and searches for the key within its own table. If the value has been captured, it can be returned; otherwise, the request will be forwarded to the peers until it is identified. From the resulting node to the initial peer which obtained the request, the reply is transmitted via the same channel in the reverse direction until it is sent to the user.

3.3.2 Self-certifying file Systems

Self-Certifying File System (SFS) is a distributed file system concept that is selfcertifying and does not require particular authorization for transferring information among nodes. Consumers receive secure access to remote files with the same rights as local files, and the transaction is completely transparent. By utilizing the public key cryptography algorithm, the IPFS system do the file self-certify that is published in network through the network. The Inter Planetary Name Space (IPNS) is a SFS integrated IPFS. Nodes can also be securely recognized through the hash of their public key (node ID), similar to the distinct hash address of files within IPFS. The nodes utilize their private keys for the signature process, meanwhile the receiver authenticate via their public keys.

3.3.3 Bitwap protocol

In IPFS, the Bitwap module protocol is applied for data trading as well as marketplace. Block exchanges across peers in the IPFS network are standard procedure. It performs two key functions such as collecting blocks that are requested through its nearby peer nodes and send every block that you possess to the peers that have requested need it.

3.3.4 Merkel DAG structure

Merkle tree given a way for authenticate data accuracy through employing the cryptography hash functionality. The topological layout of data that does not exist in cycles can be expressed using the DAG technique. Merkle DAG is an enhanced version of a Merkle tree with DAG features incorporated. It is a data structure which is utilized hashes for finding the location of the file in a DAG. Through this structure, every files or data in the system has been tamper proof that can be exclusively founded by the hash.

4. RESULTS AND DISCUSSION

The performance of the DcB assist QR system analysed through standard performance metrics such as latency, response time and throughput and so on. Also compared the performance with several existing fake drug detection system. The Python tool is used for implement the DcB assist QR system. The performance metrics description, result evaluation and discussion has been in the following sub-section

4.1 Performance Metrics

Various performance metrics are utilized for evaluating the proposed DcB assist QR system. Some of the performance metrics described as below with its mathematical equation.

4.1.1 Throughput

The rate whereby the blockchain executes authorized transactions by the several users within a given time frame is known as transaction throughput. Transaction throughput is a metric that is measured over the entire network, not just at one node.

$$T = \frac{Total\ amount\ of\ authenticated\ transaction}{Total\ time} \qquad (4)$$

Where, T represented the transaction throughput.

4.1.2 Latency

The total amount of time necessary to transport information from a single place to the next is estimated place is known as latency. The mathematical expression of the latency is given as below.

$$L_t = G_{req} + G_{consensus} + G_{responses} \qquad (5)$$

Here, the transaction request such as data transmitted to the blockchain is signified by G_{req}, the time required for the observer node to reach the consensus node is represented as $G_{consensus}$ and the whole amount of response time is denoted as $G_{responses}$.

4.1.3 Average Latency

The average Latency defined as difference among the transaction starting time and ending tine over the group of transaction.

$$Avg\_Latency = \frac{\sum_{j=1}^{m} (E_t - S_t)}{m} \qquad (6)$$

Here, transaction ending time and starting time are represented as E_t and S_t respectively, m denoted the total number of transaction.

4.1.4 Encryption time

The entire period of time needed to convert plain text into a ciphertext is known as the encryption time in cryptography algorithm.

4.2 Performance Analysis

In this paper, the DcB assist QR system is evaluated based on the several performance metrics and compared to the previous fake drug detection system. Different blockchain network performance metrics are utilized for proving the superiority of the DcB assist QR system compared to other blockchain based fake drug detection application. Figure 4 shows the throughput analysis based on the different number of user in blockchain network.

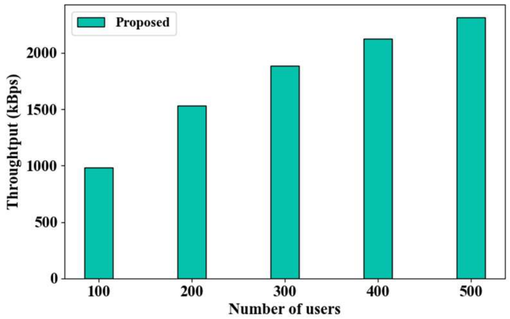

Figure 3: Analysis of throughput based on number of users

Throughput evaluation describes the amount of transaction carried out over the specific period of time by the DcB assist QR system. The high throughput is essential for best blockchain based application for more transaction done within the sort period of time. The DcB assist QR system attained 983.7 kBps throughput while the 100 number of users the block chain. Based on the number user transaction, the DcB assist QR system increase the throughput. The 500 number of user in the DcB assist QR system attained the 2312.8 kbps of throughput. So that proposed DcB assist QR transacted high amount of data with high performance. Figure 5 shows the execution time evaluation.

The blockchain utilized time for data transaction is represented the execution time. Less execution time more essential for fast transaction. The DcB assist QR system required the less time for 100,500 and 1000 transaction such as 21.05 seconds, 103.44 seconds and 210.11 seconds. The proposed DcB assist QR system provided the less execution time speed up the transaction rate so it increase blockchain network reliability and efficiency. Figure 6 represented the encryption time analysis and comparison.

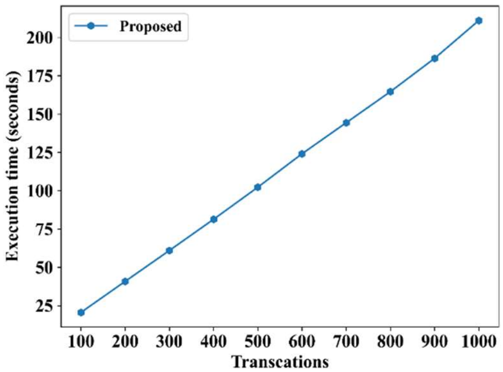

Figure 4: Analysis of throughput Execution time based on Transaction

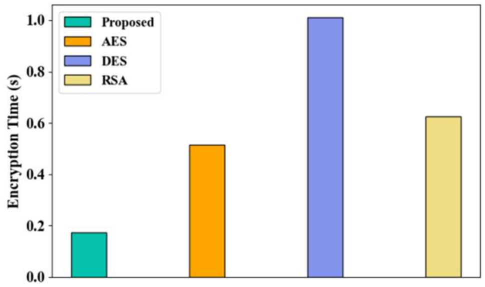

Figure 5*: Analysis and comparison of Encryption time*

The Encryption time is an important performance metrics for measuring the encryption scheme throughput. For efficient encryption techniques must provide the less encryption time. So that to know the performance of the proposed encryption techniques such as HEllC is evaluated. After that, it performance is compared with the several existing encryption techniques like Advanced Encryption Standard (AES), Data Encryption Standard (DES) and RSA (Rivest–Shamir–Adleman). The HEllC utilized 0.1837 seconds that is greatly decreased encryption time compared to other existing encryption technique. Figure 7 represented the average Latency and Throughput analysis.

Throughput and average latency are both helpful to fast and reliable network. Although latency shows how quickly a single transaction may be verified, throughput monitors the overall volume of transactions in a given period of time. The proposed DcB assist QR system attained less average latency even high throughput. If the system attained 983.7 kBps throughput then it produced only 2.708 seconds of average latency. At the same time 13.45 seconds of average latency attained 2312.8 kBps . From the evaluation the proposed system speed up load transaction and throughput with latency. Figure 8 represented the blockchain size utilized by the proposed DcB assist QR system.

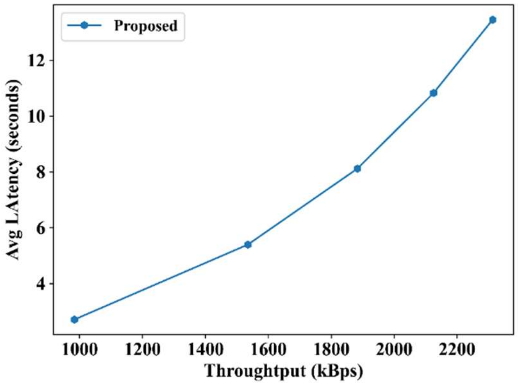

Figure 6: Analysis of average Latency and Throughput

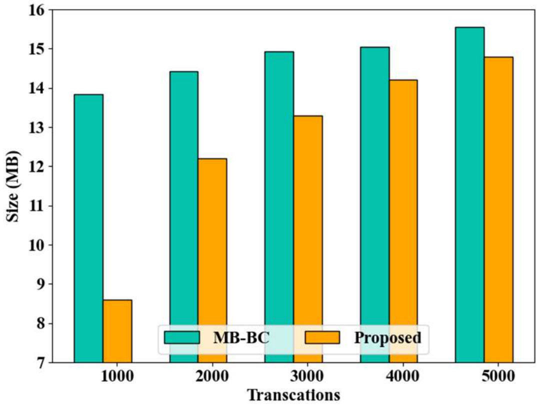

Figure 7: Analysis of utilized blockchain size based on the transaction

Blockchain system size is a one of the key measures for described the blockchain system reliability. So that, the proposed work has been evaluated based on the blockchain size performance metrics and also compared with existing system such as multi-branched blockchain scheme (MB-BC) [30]. The less blockchain size provided the high feasibility to the fake detection system. The proposed DcB assist QR system required less blockchain size such as 8.6 MB for 1000 transaction at the same amount of transaction takes 13.83 MB size by using the MB-BC system. 5000 number of transaction utilized the only 14.8 MB that effectively decreased compared MB-BC system. Figure 9 shows the latency analysis based on the transaction.

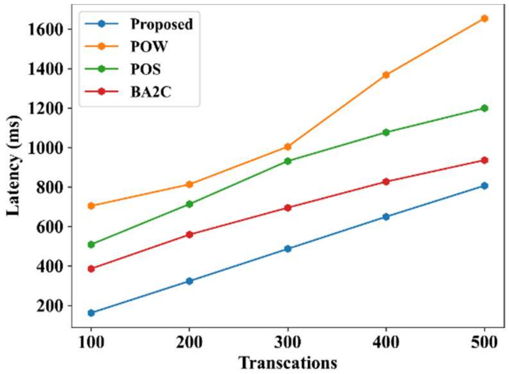

Figure 8: Analysis Of Latency Based On The Transaction

Latency is an essential performance metrics to compute the blockchain transaction time. The less latency provide fast transaction in the blockchain network. The proposed DcB assist QR system is evaluated latency based on different number of transaction. The DcB assist QR system produced the less latency such as 2.708 milliseconds compared to other existing systems such as Blockchain-based Anonymous Anti-Counterfeit (BA2C), Proof of work (POW) Proof of Stake (POS) utilized blockchain fake drug detection system [31]. From the performance evaluation, the DcB assist QR system more effectively detecting the fake drug and more securely store the medical information into the blockchain.

4.3 Discussion

The goal of the research work is fake drug detection through the QR code verification. The QR code verification some time faces the data modification issues that was solved by using the DcB assist QR system. Initially, the supply chain of the drug monitored by using the DcB assist QR system and stored into the blockchain that helpful to effectively track the drug transaction details. The limitation of the [21] is solved by attaining the 21.05 seconds of less execution time and 8.6 MB of blockchain size. The limitation of [22] is overcome by increasing the IPFS that allow to extend the node effectively. The limitation of the [23] the security of the drug details was provided by using the HEllC encryption techniques and IPBFT consensus algorithm. Limitation of the [24] is solved by DcB assist QR system that completely track the drug from the manufacturing to it collected by the patient. All the transaction details and temperature details are also stored securely into the blockchain node. The limitation of the [25] is solved through attaining the 983.7 kbps of high throughput. The DcB assist QR system only required the 0.1837 seconds of less encryption time compared to other existing techniques. So that, blockchain system speed up the encryption and user authentication process. The DcB assist QR system produced the 2.708 seconds of average latency so that blockchain system detect thee fake drug with less required time.

5 CONCLUSION

In this research work, the fake drugs are effectively detected by the DcB assist QR system. Through using the blockchain, the medicine details and supply chain details are securely stored. So that, the medicine details is cannot accessed by any intruders over the network. The blockchain security is increase by using the encryption techniques and authentication techniques. The DcB assist QR system uses the HEllC encryption algorithm for secure the data during the transaction. The user are authenticated by using the IPBFT, so that unauthorized users cannot access the confidential medicine data and also cannot modify the derails. During drug transportation, the temperature monitoring of drugs is done by IoT sensors and whenever temperature crosses the threshold, the alert message is send to the driver of the vehicle. That helpful to know manually exchange done during the transportation. Finally, an IPFS was employed to store drug temperature data in a decentralized way. Moreover, the performance of the DcB assist QR system evaluated based on various several performance metrics and compared to existing system. The DcB assist QR system attained 21.02 seconds of less execution time, 2.708 milliseconds of Latency and 983.7 kBps of throughput. In future work, enhanced the reward and trust mechanism in the blockchain system for improving the security of the drug details.

REFERENCES

[1] P. Pandey and Ratnesh Litoriya. "Securing e-health networks from counterfeit medicine penetration using blockchain." *Wireless Personal Communications* Vol. 117 (2021): 7-25.

[2] R. Kumar and Rakesh Tripathi. "Traceability of counterfeit medicine supply chain through Blockchain." In *2019 11th international conference on communication systems & networks (COMSNETS)*, pp. 568-570. IEEE, 2019.

[3] K. Abbas, Muhammad Afaq, Talha Ahmed Khan, and Wang-Cheol Song. "A blockchain and machine learning-based drug supply chain management and recommendation system for

smart pharmaceutical industry." *Electronics* Vol. 9, no. 5 (2020): 852.

[4] A. Musamih, Khaled Salah, Raja Jayaraman, Junaid Arshad, Mazin Debe, Yousof Al-Hammadi, and Samer Ellahham. "A blockchain-based approach for drug traceability in healthcare supply chain." *IEEE access* Vol. 9 (2021): 9728-9743.

[5] W. J. Chang Liang-Bi Chen, Chia-Hao Hsu, Cheng-Pei Lin, and Tzu-Chin Yang. "A deep learning-based intelligent medicine recognition system for chronic patients." *IEEE Access* Vol. 7 (2019): 44441-44458.

[6] Z. Zhao, Yangmyung Ma, Adeel Mushtaq, Abdul M. Azam Rajper, Mahmoud Shehab, Annabel Heybourne, Wenzhan Song, Hongliang Ren, and Zion Tsz Ho Tse. "Applications of robotics, artificial intelligence, and digital technologies during COVID-19: a review." *Disaster Medicine and Public Health Preparedness* Vol. 16, no. 4 (2022): 1634-1644.

[7] P. Zhu, Jian Hu, Yue Zhang, and Xiaotong Li. "A blockchain based solution for medication anti-counterfeiting and traceability." *IEEE Access* 8 (2020): 184256-184272.

[8] Y. Liu, Fei Han, Fushan Li, Yan Zhao, Maosheng Chen, Zhongwei Xu, Xin Zheng et al. "Inkjet-printed unclonable quantum dot fluorescent anti-counterfeiting labels with artificial intelligence authentication." *Nature communications* Vol. 10, no. 1 (2019): 2409.

[9] J. Chen, Kenli Li, Zhaolei Zhang, Keqin Li, and Philip S. Yu. "A survey on applications of artificial intelligence in fighting against COVID-19." *ACM Computing Surveys (CSUR)* Vol. 54, no. 8 (2021): 1-32.

[10] S. Kulkarni, Nuran Seneviratne, Mirza Shaheer Baig, and Ameer Hamid Ahmed Khan. "Artificial intelligence in medicine: where are we now?." *Academic radiology* Vol. 27, no. 1 (2020): 62-70.

[11] C. Antal, Tudor Cioara, Marcel Antal, and Ionut Anghel. "Blockchain platform for COVID-19 vaccine supply management." *IEEE Open Journal of the Computer Society* Vol. 2 (2021): 164-178.

[12] E. Noviana, Daniel Blascke Carrão, Rimadani Pratiwi, and Charles S. Henry. "Emerging applications of paper-based analytical devices for drug analysis: A review." *Analytica chimica acta* Vol. 1116 (2020): 70-90.

[13] F. Firouzi, Bahar Farahani, Mahmoud Daneshmand, Kathy Grise, Jaeseung Song, Roberto Saracco, Lucy Lu Wang et al. "Harnessing the power of smart and connected health to tackle COVID-19: IoT, AI, robotics, and blockchain for a better world." *IEEE Internet of Things Journal* Vol. 8, no. 16 (2021): 12826-12846.

[14] G. Subramanian, Anand Sreekantan Thampy, Nnamdi Valbosco Ugwuoke, and Baghwan Ramnani. "Crypto pharmacy–digital medicine: A mobile application integrated with hybrid blockchain to tackle the issues in pharma supply chain." *IEEE Open Journal of the Computer Society* Vol. 2 (2021): 26-37.

[15] M. S. Al-Zahrani, Heider AM Wahsheh, and Fawaz W. Alsaade. "Secure real-time artificial intelligence system against malicious QR code links." *Security and Communication Networks* 2021 (2021): 1-11.

[16] N. Saxena, Ieuan Thomas, Prosanta Gope, Pete Burnap, and Neeraj Kumar. "Pharmacrypt: Blockchain for critical pharmaceutical industry to counterfeit drugs." *Computer* Vol. 53, no. 7 (2020): 29-44.

[17] V. Mishra, Dhiraj Aswani, Juhi Mulchandani, and Sahil Sadhwani. "Pharmaledger-An Improved Solution to identify counterfeit drugs in Supply Chain."

[18] V. Kamath, Yaparla Lahari, and Kusuma Mohanchandra. "Blockchain based framework for secure data sharing of medicine supply chain in health care system." *International Journal of Artificial Intelligence* Vol. 9.1 (2022): 32-38.

[19] M. M. Akhtar and Danish Raza Rizvi. "Traceability and detection of counterfeit medicines in pharmaceutical supply chain using blockchain-based architectures." *Sustainable and energy efficient computing paradigms for society* (2021): 1-31.

[20] N. Alam, Md Rabiul Hasan Tanvir, Sadah Anjum Shanto, Fateha Israt, Aysha Rahman, and Sabrina Momotaj. "Blockchain based counterfeit medicine authentication system." In *2021 IEEE 11th IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, pp. 214-217. IEEE, 2021.

[21] S. K. Nanda, Sandeep Kumar Panda, and Madhabananda Dash. "Medical supply chain integrated with blockchain and IoT to track the logistics of medical products." *Multimedia Tools and Applications* (2023): 1-23.

[22] M. Uddin, "Blockchain Medledger: Hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry." *International Journal of Pharmaceutics* 597 (2021): 120235.

[23] A. Musamih, Khaled Salah, Raja Jayaraman, Junaid Arshad, Mazin Debe, Yousof Al-Hammadi, and Samer Ellahham. "A blockchain-based approach for drug traceability in healthcare supply chain." *IEEE access* 9 (2021): 9728-9743.

[24] G. Khalil, Robin Doss, and Morshed Chowdhury. "A novel RFID-based anti-counterfeiting scheme for retail environments." *IEEE Access* 8 (2020): 47952-47962.

[25] H. M. Garcia, Manuel Maza Cortez, and Edgar Diaz Amaya. "Blockchain-based Website Solution for Controlling the Authorized Sale of Drugs in Peru." In *2020 IEEE Engineering International Research Conference (EIRCON)*, pp. 1-4. IEEE, 2020.

[26] P. Pandey and Ratnesh Litoriya. "Securing e-health networks from counterfeit medicine penetration using blockchain." *Wireless Personal Communications* 117 (2021): 7-25.

[27] S. Ullah, Zheng Jiangbin, Muhammad Tanveer Hussain, Nizamud Din, Farhan Ullah, and Muhammad Umar Farooq. "A perspective trend of hyperelliptic curve cryptosystem for lighted weighted environments." *Journal of Information Security and Applications* 70 (2022): 103346.

[28] G. Navaroj, Indra, E. Golden Julie, and Y. Harold Robinson. "Adaptive practical Byzantine fault tolerance consensus algorithm in permission blockchain network." *International Journal of Web and Grid Services* 18, no. 1 (2022): 62-82.

[29] G. Subathra, A. Antonidoss, and Bhupesh Kumar Singh. "Decentralized Consensus Blockchain and IPFS-Based Data Aggregation for Efficient Data Storage Scheme." *Security and Communication Networks* 2022 (2022).

[30] X. Tan, Zerui Kang, Fan Wei, Chenhao Gao, Zhaoying Wei, and Haiping Huang. "MB-BC: drug traceability system based on multibranched blockchain structure." *Wireless Communications and Mobile Computing* 2022 (2022).

[31] N. Anita, M. Vijayalakshmi, and S. Mercy Shalinie. "Blockchain-based anonymous anti-counterfeit supply chain framework." *Sādhanā* 47, no. 4 (2022): 208.