Fuzzy Systems and Soft Computing
ISSN : 1819-4362

ENSURING TRACEABILITY AND MONITORING OF MEDICAL DEVICES WITH NFTS AND BLOCKCHAIN

#1NUKALA KAVYA SRI,
#2PADMARAP DEEPIKA,
#3PEDDI KISHOR, ***Associate Professor,***
Department of Computer Science and Engineering,
SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, TS.

ABSTRACT - Quality and safety are very important for medical devices because they have a big effect on people's lives and health. It is common for fake goods to be made because the copied product is cheaper. Due to the high risk, it is very important to set up a traceability system. Most businesses are stepping up their efforts to stop counterfeiting. A QR code system for applications, security, and privacy is being introduced by this project. suggests that medical devices be tracked with QR codes and blockchain technology. Putting together blockchain technology (which is decentralized and can't be changed) with traditional tracing systems made the alliancechain and smart contract construction system possible.QR codes are an easy and inexpensive way for businesses and customers to check that a device works properly.Making an identification device with a QR code is easy and doesn't cost much.In the proposed system, QR codes are used. These are easy to set up.This study doesn't use third-party apps to check the legitimacy of medical devices. Instead, it uses a distributed blockchain technology system. Blockchain is a decentralized ledger system that securely stores and records data from medical devices. Strong cryptography technology was used to build it.Lastly, and most importantly, use the Data Encryption Standard (DES) algorithm to encrypt information about how you bought a health device.

KEYWORDS: Secure Medical,DeviceInformation, QRCodeGeneration, BlockchainTechnology,Authenticity Verification, Medical device purchase, DES Encryption.

I.INTRODUCTION

The introduction of QR codes created a wave of opportunity for the technology sector by enabling precise and fast data and information retrieval from any location. When you visit a website or app, you have the option to engage with it. With the rise in mobile devices, QR code technology emerged as a crucial means of instantaneous two-way communication, networking, and information sharing [4]. It is also a secure method of information sharing because, in the absence of appropriate tools, it is impossible to obtain data that isn't intended for public consumption. The blockchain will become even safer when QR codes are added.

BLOCKCHAINTECHNOLOGY

Blockchain, a peer-to-peer network technology, allows users to see and access trusted data even in situations where users don't know or trust one another. By storing unchangeable encrypted copies of transaction records on each network node, it safeguards their accuracy and decentralization. To incentivize users who strengthened the network against collusion and attacks, native network tokens were implemented . The Internet gains a layer of open, international accounting and governance from blockchain and related technologies. Every user on the network has equal access to the same data in real time. Every member of the network is able to see and comprehend the origins of transactions. Blockchain can also be compared to an open-source distributed accounting system and a supranational governance apparatus. A transaction is added to the blockchain permanently once it is approved by the majority of the network. Should you fail to fulfill any of these prerequisites, the transaction will be refused. A transaction must be added to the blockchain in order for it to be regarded as legitimate and irreversible.

The "blockchain," also known as the distributed ledger, is a system for recording transactions. No single user has control over it, but all users can access it. A distributed database that uses encryption to prevent changes and tampering maintains the collection of records containing transaction data. Blockchain comes in three flavors : consortium, private, and public. With public blockchains like Ethereum and Bitcoin, anyone, anywhere, at any time, can join the demand and receive assistance. Complex mathematical functions illustrate this. Similar to decentralized ledgers, private blockchains operate. The organization owns the blockchain, which is accessible to users. Building blocks and mining occur much more quickly on private blockchains than on public ones because they have fewer nodes than public blockchains. A consortium, on the other hand, consists of several companies that collaborate to manage a blockchain system. In order to regulate blockchain transactions, membership rules perform better than consensus. The research is being conducted using the Consortium blockchain, and it will be overseen by a national authority in the nation. The blockchain's most crucial component is the block. A block is composed of two parts: the header and the body. The transactions that the system writes comprise the latter. Information about the block, including the time stamp, transactions, difficulty, nonce value, and previous hash, is contained in the block header. The block size was stated to be either one megabyte or eight megabytes. A special method for locating the block that needs to be placed is through the block header.

HASHING

A fixed size output can be obtained by hashing any size input. Some functions have multi-level hashing capabilities. The MD5 algorithm is particularly helpful in the hashing field because of its 32-character width and 128-bit hash value. The MD algorithm family has five new versions: MD4, MD2, MD3, and MD5. The algorithm was initially designed as a cryptographic hashing algorithm, but because of its current flaws, it is not as effective at producing unique hashes. An additional cryptographic hash algorithm called SHA generates a 160-bit hash value using 40 hexadecimal characters. The algorithm has lost favor because it cannot withstand collusion attacks. A number of new algorithms, including SHA3 and SHA256, have recently become available. The US-based National Security Agency is responsible for developing the SHA2 algorithms. For the time being at least, it is believed that the new hash functions, SHA256 and SHA512, are secure and free from collusion issues.

In a blockchain, every block must have a unique set of headers.

PreviousHash:

You can find out what block came before it with this address.

TransactionDetails:

The necessary transactions must be identified.

Nonce:

a random number that can be used to distinguish between block hashes in cryptography.

Hash AddressoftheBlock:

A hashing algorithm is then used to send the aforementioned data along with the transaction details and nonce. This produces an output with the distinct "hashaddress," a 64-character, 256-bit value. The block hash is the hash value that is discovered. Computer algorithms are used by a large number of people worldwide in an attempt to determine the ideal hash value that satisfies a given set of requirements. The transaction is deemed complete when the predetermined condition is satisfied. Solving the mathematical puzzle known as the proof-of-work problem is the primary objective of blockchain mining. There will be prizes for the first person to solve it.

Mining

Although "mining" is frequently connected to Bitcoin, it can also be applied to other blockchain systems. The process of adding transaction details to the public digital ledger in blockchain technology is known as "mining." Mining produces a hard-to-forge hash of a block transaction, protecting the entire decentralized Blockchain system.

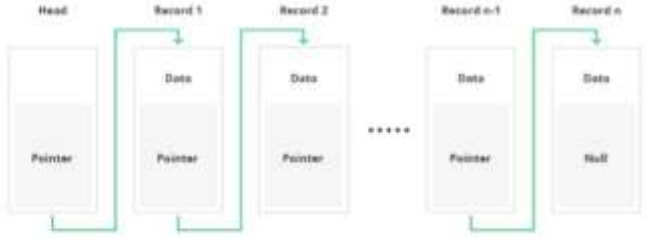

Fig 1: BlockCreation

II.RELATEDWORK

AFarhadAghiliaetal, Developed an energy-efficient and secure protocol that accomplishes the aforementioned objectives, including access control, key agreement, user authentication, and privacy protection for both patients and doctors. In addition, for the first time, consideration is being given to the transfer of user ownership. Changes to the ownership of patient data may occur on the medical server throughout the ownership transfer phase of the proposed scheme. Additionally, security vulnerabilities discovered in earlier authentication protocols for e-health systems are patched by the LACO protocol. Traceability issues, desynchronization, insider attacks, and DoS attacks were among the risks that these protocols might encounter. In order to mitigate the recurrence of similar errors, a comprehensive security analysis, both formal and informal, was conducted on the ProVerif language utilized in the LACO protocol. By doing so, we ensure that the suggested framework is impervious to the most prevalent vulnerabilities that may impact IoT systems. The proposed authentication and key agreement protocol grants users greater control over who can view content and facilitates their ability to maintain anonymity. Moreover, LACO, the proposed protocol, is capable of managing ownership transfers between physicians and patients. If it becomes necessary to change the owner of a user or a physician under the LACO scheme, the medical server facilitates the ownership transfer process. One of the primary initiatives addressing the issue of how to transfer ownership of Internet of Medical Things (IoMT) systems from patients to physicians is the LACO initiative. By examining the functionality and security of LACO, the proposed method demonstrated that the scheme could and would remain secure for implementation in IoMT systems.

Raja Wasim Ahmad et al, It was proposed that a distributed ledger system (blockchain) be implemented to facilitate the sharing of trustworthy, traceable, and transparent information and to accelerate the supply chain for all parties involved in managing the waste of COVID-19 medical equipment. The proposed method combines the Ethereum blockchain with the decentralized storage system IPFS in order to securely retrieve, store, and distribute information regarding the forward supply chain and the disposal of COVID-19 medical equipment. Develop algorithms that illustrate optimal stakeholder interactions with COVID-19 waste, as well as the repercussions of failing to adhere to these guidelines. The proposed strategy may potentially assist the government in ensuring that COVID-19 testing facilities dispose of COVID-19 medical waste and treat COVID-19 patients with the appropriate medical equipment. This document contains an exhaustive cost analysis that demonstrates the rationale behind the proposed method. The SmartCheck program was employed to assess the proposed method for established security vulnerabilities. The proposed method is flexible and can be modified rapidly to accommodate a vast array of use cases. Everyone has access to the complete code for the proposed implementation on GitHub.

Abirami Raja Santhi et al.,Compiled, evaluated, and reviewed the literature in order to provide a comprehensive picture of the potential supply chain and logistics applications of blockchain technology. Blockchain technology has the potential to revolutionize supply chains and logistics by making them more transparent, secure, flexible, and dependable, according to the study. An essential distinction that sets blockchain networks apart from conventional databases such as MySQL is the manner in which ledgers and transactions are stored. A case study application scenario is developed to illustrate the advantages of blockchain technology in terms of tracing and validating the provenance of critical products. Blockchain technology is characterized by its decentralized nature, immutability, and dispersion. Due to the centralized nature of databases, it is possible for an administrator to modify the data contained within. Additionally, cyberattacks may compromise the entire database. The decentralized nature of a blockchain network, on the other hand, grants each node the ability to observe and record every transactional detail. Consequently, irrespective of the blockchain's privacy setting, all network nodes are obligated to authenticate transactions and append timestamps to the data transmitted within blocks.

Thomas K, et.al,Considerable scholarly investigation has been devoted to the technical aspects of numerous SC traceability systems that employ blockchain technology . The literature was categorized in this study according to several standards: the sustainability perspective that these implementations share (including economic, environmental, and social issues); the level of development of these systems' implementations, including any technical challenges; and the relevant methodologies and system types that are currently utilizing blockchain technology to enable SC traceability. This approach provides valuable insights into the existing challenges and obstacles associated with the integration of traceability into blockchain technology, in addition to potential avenues for future research. Considering the expenses and restricted efficacy of SC, it is evident that pragmatic approaches to tracking must be devised and evaluated. Although blockchain technology has the potential to be applied to a wide range of SC traceability solutions, unstructured experimentation has historically been favored in academia.

Muhammad Azeem Akbar, et.al Developed a healthcare blockchain maturity model (MMBH) for implementing blockchain technology in healthcare systems, based on best practices, critical barriers (CBs), and key success factors (CSFs). The initial findings of an SLR to identify CSFs for blockchain implementation in healthcare systems are presented in this article. This constitutes the initial phase in the construction of the MMBH. Fuzzy TOPSIS was additionally employed to rank the identified CSFs. Initial efforts to address these concerns and identify critical success factors that will accelerate the adoption of blockchain technology in healthcare could be the objective of the proposed study. Academics and industry professionals have discussed the concept of an MMBH. This is a novel and significant study because prior to this one, no one had attempted to provide a road map for resolving blockchain implementation issues. Fuzzy-TOPSIS analysis was employed to rank the identified success factors in this experiment. It is possible to use the proposed model by applying it to a case study. The research results have a lot of real-world implications.

M.M.Kamruzzaman,et.al,…A comprehensive literature review demonstrating the impact of fog, blockchain technology, and the Internet of Things (IoT) on healthcare systems and practices in smart cities was delineated in a framework published in [6]. Due to the paucity of pertinent data, ten studies were selected for examination, and their findings were meticulously assessed. Among the three technologies examined, the smart city healthcare sector has made the most extensive use of the Internet of Things (IoT), according to the systematic review. Typically, a "smart city" refers to an urban region equipped with state-of-the-art electronic communication and data storage infrastructures that facilitate the transmission and reception of information. The integration of information and communication technologies expedites and reduces the expense of information sharing. The Internet of Things (IoT), fog computing, and blockchain, for instance, could automate tasks in smart cities and assist healthcare. They will be extremely beneficial within the framework of smart cities and smart initiatives. An Internet of Things (IoT) is a network of interconnected computers capable of exchanging information and communicating. The blockchain is an immutable, decentralized ledger composed of interconnected blocks. A public ledger and a distinct representation of a transaction are associated with each block. Fog computing concludes with a virtual platform bridging the gap between the client computer and the cloud center.

Kazi Tamzid Akhter Md Hasib, et.al,…There is... Blockchain technology was employed to establish a mechanism for monitoring the online exchange of health records. The primary objectives are to strengthen data security and increase the level of difficulty for unauthorized individuals to access medical records. We can expedite and save time by documenting the procedures. The greatest advantage is that consumers will feel more secure when making purchases. The implementation of peer-to-peer technology and smart contracts occurred. By utilizing an immutable ledger, this system effectively restricts access to authorized individuals. Once granted access to the system, they will be unable to modify any data. You will receive a full refund for every purchase made, excluding damaged items. Security for transactions is a viable substitute for employing cryptography as a solution to these issues. The utilization of blockchain technology by this website to safeguard medical data will benefit both physicians and patients. Physicians and patients are distinct entities. A patient's profile can be generated through the input of their distinct postal code, complete name, and age. A unique address will subsequently be assigned to this profile; this address will be extracted from the genesis block. The proposed network will ensure the privacy and security of the proprietor with regard to this distinct address. The patient can view a list of physicians and upload medical records such as X-rays and prescriptions after creating an account. Local server storage will be utilized for all patient records.

SuyelNamasudra,,et.al,…A proposed approach leverages blockchain technology and mobile applications (MA) to establish a secure configuration for internet of things-connected healthcare systems. Security and protection against unauthorized access to medical certificates are both enhanced by the proposed system. It expedites the verification process of physical certificates and prevents unauthorized access to birth, death, and sick leave records. A blockchain-based application for generating and overseeing medical certificates on Internet of Things (IoT) devices is proposed in this study. The Proof of Stack consortium algorithm and the Ethereum public blockchain network are both utilized by the proposed system. InterPlanetary File System (IPFS) is utilized for certificate storage and remembrance. Once the certificates have been stored, IPFS generates a distinct transaction ID and hash. Users of MA were issued a one-of-a-kind ID that they may display or consult whenever necessary to access the appropriate certificate.

Kebira Azbeg, et.al Demonstrated a blockchain-based system for securing the communication between healthcare IoT devices. The proposed solution seeks to enhance patient privacy protection while concurrently ensuring the secure collection, storage, and sharing of medical records among healthcare teams. Since blockchain technology is decentralized, it might be able to safeguard against a potential vulnerability. Smart contracts also enable the authentication of devices in a secure manner and the regulation of data access. It consists of proxy re-encryption, the Interplanetary File System (IPFS), blockchain technology, smart contracts, and Internet of Things (IoT)-connected medical devices. Prior to being stored in an off-chain database, health information undergoes a secret IPFS encryption process. This bolsters the case for a scenario-based diabetes management system that monitors diabetic patients remotely in a secure manner. In contrast to the most cutting-edge techniques presently operational, the system under consideration provides an exceptionally elevated standard of security. An online version of the proposed solution is currently under development. Subsequent investigations will focus on the application of fog layers to filter data prior to its transmission from medical devices to hospitals. It is also capable of analyzing data in real time and providing patients with the results.

Ammar Odeh, et.al,The researchers in conducted an extensive examination of the potential applications of blockchain technology in the fields of healthcare and medicine, with a specific emphasis on the distinctive challenges and prospects it presents. Specialized applications include patient monitoring, electronic health records (ERH), and medication tracking. Maintaining confidentiality is a fundamental ethical tenet. Trust is the only element that sustains the relationship between a patient and an expert within the healthcare system. Therefore, the foundation of all medical records must be the trust that healthcare professionals, including physicians, will consistently maintain the confidentiality of the information entrusted to them (e.g., patients). This information must remain confidential and not be disclosed to unauthorized individuals or family members, unless required to do so by law or with the patient's written consent. We can conclude, based on the information contained in any of these sources, that blockchain technology has not been effective in protecting data from unauthorized parties. This contradicts the prevalent notion among educators that patient medical records ought to be securely stored at all times.

III. EXISTING METHODOLOGIES

In order to create a secure and efficient way to track who owns medical devices and how they are used, the current framework recommends using a non-fungible token (NFT) solution that includes blockchain smart contracts, tokenization protocols, and a decentralized storage infrastructure. NFTs refer to the digital replica of the physical device in the proposed system. From the moment a medical device is conceived to the moment it is owned, its entire life is tracked by this digital twin. Before using the system, all participants must register and provide identification through the necessary application. NFTs do not disclose the owner's identity; they only disclose the wallet address. This is a crucial first step because the proposed system requires participant identification before selling and delivering actual medical devices. This is simple to accomplish when utilizing a private blockchain: all users need to do is wait for an invitation to join the network and complete the required documentation. On the other hand, entities or individuals in a public blockchain can be verified to be where they claim to be using digital certificates.

Digital certificates can be used for registration and authentication as well. By submitting digital certificates, users will be able to verify and validate the identities of stakeholders if the suggested system is implemented on a public blockchain. The NFT metadata must be provided by an authorized user prior to a medical device being sold. This consists of an authenticity certificate based on IPFS and a hashed copy of the device's digital twin. To verify that a technical device is genuine or unique, one needs a certificate of authenticity (COA), a legitimate document issued by the manufacturer or a recognized third-party certificate provider. The COA is digitally signed via the DApp with the manufacturer's private key—a cryptographic value used for data encryption—to reassure customers. Technical details about the device, such as its name, unique ID, and manufacturing process, should be included in the COA template.

Details about the writer. The next stage is to create a token certificate on the blockchain that represents the actual medical device and store it there. Device manufacturers, regulatory agencies such as the FDA, and certification service providers are all able to verify the information, approvals, and certifications that were submitted thanks to the NFT contract. NFT metadata is created and saved by the smart contract in an open repository called IPFS. The NFT medical device can be purchased by anyone who has registered using the DApp. The buyer owns the NFT as soon as the transaction is approved. The blockchain records the transaction and notifies all parties involved of it.

IV.MEDICALDEVICETRACKINGUSINGQRCODEWITHBLOCKCHAINSTORAGEANDDESENCRYPTION

Medical devices have the potential to impact people's lives and health, everyone understands how crucial it is for them to be reliable and safe. The goal of this proposed work is to create a legitimate system for purchasing medical devices by combining blockchain and QR code technology. Depending on its importance, a traceability system may or may not be required. Medical device tracking offers numerous advantages, including a reduction in medical errors and the elimination of phony or subpar medical supplies from the marketplace. Additionally, it helps companies track the location of a specific product batch, safeguard the rights of their customers, and identify the root of the issue. This project aims to develop a blockchain-based medical device tracking system. A decentralized medical device tracking system is constructed using distributed storage, encryption, a blockchain consensus mechanism, and additional technological elements. This system performs well in handling issues such as unidentified data sources and malicious users manipulating data in intermediate links. Manufacturers, distributors, hospitals, and consumers are among the parties that can view a product's complete lifecycle and obtain information about it. By scanning the QR code, customers can quickly obtain the information they require. Consumers can use QR codes to obtain details about a product, including its cost, maker, availability, and manufacturing duration.

Checked-out members ensure that the authorization, monitoring, and distribution of medical devices follow a secure and trustworthy protocol. Initially, manufacturers of medical devices maintain records about them. The chain manager keeps an eye on this data, which is stored in a "block" of the blockchain. When a manufacturer ships the first batch of medical devices and the seller receives them, data is entered into an unchangeable ledger using blockchain technology. Every node in a medical device information system collaborates with others to ensure the integrity of the system and to execute decisions. A few nodes being attacked and then taken offline won't have any effect on the blockchain system as a whole. When medical device manufacturers can track their products at every stage of the supply chain, their customers are more likely to believe in them. However, the buyer will know that the product they are purchasing is authentic and manufactured by a reliable business. The manufacturer of the product guarantees that the goods will reach the client in a secure manner. Data about a medical device can be traced from the manufacturer to the buyer when it is purchased through standard channels. This feature can be made available to users of the medical device information system by incorporating blockchain technology. This would enable the system to record each time a patient purchased a medical gadget.

V.METHODOLOGY

QRCODE GENERATION

Quick Response (QR) codes are scanned barcodes used to store data. An entity adopts a specific format when it is encoded. A unique two-dimensional square grid with kanji, byte, alphabetic, and numeric characters makes up a Quick Response (QR) code. The optical scanner rotates through the squares, rearranging the arrangement from the beginning.

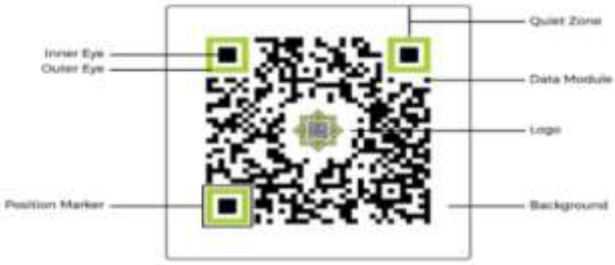

Fig2:QRCodeStructure

Several crucial components of a QR code are:

Datamodule.

The ideal color scheme for creating a personalized QR code is black on white, but you can also experiment with different contrast levels and color schemes. This QR code reader is standard. The standard design element is a white square with black text inside of it. A QR code is created by arranging these black squares, which are data modules, in the correct sequence.

Position marker.

There are three built-in locators in every QR code. Because they have both an internal and an external eye, scanners and cameras can locate data modules and scan directions with speed and accuracy.

Quiet zone.

In this instance, the data modules and position markers are arranged to form a matrix with empty spaces surrounding it. The beginning and end of a QR code can now be distinguished by readers and scanners.

BLOCKCHAINTECHNOLOGY

Digital data storage is now a reality thanks to blockchain technology.There is no way to modify the data once these blocks are connected.Data can be altered in various ways once it is linked to another block.Regardless of whether it is added to the blockchain or not, it will remain accessible to the public in the same manner as before.

(Secure Hash Functions 1, 2, and 256) Most blockchain users prefer encryption as their primary secure algorithm due to the reliability of its hash function. When various inputs are provided, it generates distinct outputs. An integral aspect of the petroleum supply chain, the hash function generates a one-of-a-kind key that can be utilized for both identity verification and transaction completion [19].

The capacity of blockchain technology to convert bits of a fixed size into strings of characters makes it feasible to construct a robust and efficient hashing algorithm.Each proposed transaction is hashed in a blockchain before being added to a block. By connecting each block to the one that came before it, hash pointers ensure that previous hash data is always stored. Every block in the blockchain is affected by the hashing algorithm, so any change to that algorithm will result in new hash strings with different characters .

BlockandHashGeneration

- A block that records details of ongoing transactions.
- Ultimately, every data point generates its unique hash.
- It displays a combination of letters and numbers.
- The chronological order of recorded transactions remains unchanged throughout the entry process.
- In order to get the hash, we add up the hashes of all the transactions that have occurred up to this point.
- All modifications to a transaction trigger the creation of an additional hash.
- To verify the legitimacy of a transaction, the nodes check its hash.
- To be included in a block, a transaction needs the approval of most nodes. All of the blocks in the blockchain are connected to one another.
- A blockchain is distributed ledger that is maintained by multiple computers, or nodes, with a copy of the blockchain stored on each node.

DES CERYPTOGRAPHY

The Data Encryption Standard (DES) algorithm requires a specific length of plaintext as input and returns a ciphertext of the same length, allowing for the creation of symmetric encrypted data. This is how the DES algorithm is implemented.

Key Generation:

A 64-bit encryption key can be generated from a user-supplied passphrase using a key derivation function. The encryption and decryption processes both require this key.

InitialPermutation:

Changing the sequence of the 64-bit plaintext block using a fixed permutation table.

Splitting:

Two 32-bit blocks, the left half and the right half, comprise the permuted plaintext.

RoundFunction:

Every one of the sixteen rounds followed these procedures:

Expansion:

Using an expansion table increases the width of the right half of the plaintext from 32 bits to 48 bits.

KeyMixing:

A subkey with 48 bits is XORed with the expanded right half of the present encryption key.

Substitution:

After the 48-bit output is divided into 86-bit chunks, each chunk is further expanded to 84 bits by adding an S-box table.

Permutation:

To randomly select the 32-bit result of the replacement operation, a table of fixed permutations is utilized.

Mixing:

Combine the modified output with the left half of the original plaintext using the XOR operator.

FinalPermutation:

The plaintext is split in half and rearranged according to a predetermined table sixteen times to produce the final ciphertext.

An outline of the DES algorithm has been provided by the steps that have been performed thus far. Variations on DES that aim to improve security include key fortification, multiple encryptions, and others. More recently developed encryption algorithms such as AES have largely superseded DES.

VI.PROCEDURE

AdminCredentials

Distributors, patients, and manufacturers can all benefit from a more secure medical device supply chain thanks to blockchain technology. A complete audit trail of medical device supply chains can be found on the blockchain. Looking at the manufacturer's company certificates allows the administrator to verify their credentials. The administrator can initiate the process by logging in, which requires multiple authentication factors.

MedicalDeviceDetailswithQR

Here is where medical device makers can upload data to the application server. As part of the registration procedure, you can scan the QR code and include it with each collection of data pertaining to the medical device. A unique QR code was assigned to each medical device during the registration process. Using this function, the whole supply chain can see products in their proper categories. The blockchain will also include details regarding that medical device.

BlockchainCreation

The manufacturer of the medical device attaches a one-of-a-kind QR code to it. The medical device's production details and QR code are both recorded on the blockchain. All participants in the supply chain have access to the complete picture thanks to the manufacturer data stored on the blockchain. Every transaction is associated with a unique hash ID that is then added to the blockchain. This makes it much easier to monitor transactions.Medical device manufacturers will initially be responsible for record keeping.A manager monitors the data stored on the blockchain, which is structured into "blocks." Using blockchain technology, it ensures that all information pertaining to medical devices, from the initial batch sent by the manufacturer to the final batch received by the seller, is recorded in an immutable manner. Every node in an MDS collaborates with others to execute decisions and maintain the integrity of the system.

InformationTracking

Medical device purchases and tracking are made possible through the integration of blockchain technology and QR codes, which allows for faster, safer, and more accurate processes. A unique Quick Response (QR) code can be assigned to each medical device. This code can include crucial information such as the batch number, maintenance record, production date, and expiration date. By simply scanning the QR code with their phones, medical professionals can confirm the device's authenticity.

MedicalDevicePurchase

Medical device manufacturers can receive direct payments from healthcare providers using a blockchain-based payment system.Eliminating intermediaries and facilitating transparent and secure transactions are two benefits of this system. By closely monitoring the use and maintenance logs, medical professionals can ensure that the devices are functioning properly and reduce the likelihood of their breaking. The proposal proposes encrypting purchase data using the DES algorithm. The confidentiality of any information pertaining to the purchase of medical devices is guaranteed by these measures.

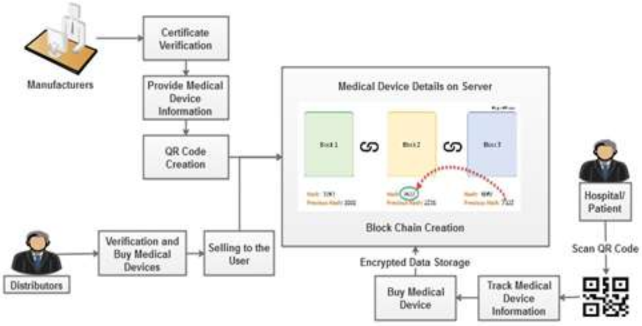

Fig3:ArchitectureforProposedWork

VII.CONCLUSION

In order to prevent the purchase of counterfeit or otherwise unlawful goods, the proposed system would enable consumers to quickly and easily verify the manufacturer's credentials. Since the origin data recorded in blockchain cannot be altered, a product that has been QR code validated is believed to be authentic. Without relying on a central server, this Blockchain Ledger can record product information and detect instances of tampering, cloning, and tag replication. These are not to be reused. Keep in mind that technical solutions alone will not put an end to counterfeiting. It is also important to have an effective alert system, use airtight packaging, educate the public, and take legal action against counterfeiters.

REFERENCES

1. Aghili, Seyed Farhad, Hamid Mala, Mohammad Shojafar, and Pedro Peris-Lopez. "LACO: Lightweight three-factor authentication, access controland ownership transfer scheme for e-healthsystemsinIoT."future

generationcomputer systems 96 (2019): 410-424.

2. Ahmad, Raja Wasim, Khaled Salah, Raja Jayaraman, Ibrar Yaqoob, Mohammed Omar, and Samer Ellahham. "Blockchain-basedforwardsupplychainandwastemanagementforCOVID-19medicalequipmentandsupplies."IeeeAccess 9(2021):44905- 44927.
3. RajaSanthi,Abirami,andPadmakumarMuthuswamy."Influenceofblockchaintechnologyinmanufacturingsupplychainand logistics." Logistics 6, no. 1 (2022): 15.
4. Dasaklis, Thomas K., Theodore G. Voutsinas, Giannis T. Tsoulfas, and Fran Casino. "A systematic literature review of blockchain-enabled supply chain traceability implementations." Sustainability 14, no. 4 (2022): 2439.
5. Akbar, Muhammad Azeem, Víctor Leiva, Saima Rafi, Syed Furqan Qadri, Sajjad Mahmood, and Ahmed Alsanad. "Towards roadmaptoimplementblockchaininhealthcaresystemsbasedonamaturitymodel." JournalofSoftware:Evolutionand Process (2022): e2500.
6. Kamruzzaman,M.M.,BingxinYan,MdNazirulIslamSarker,OmarAlruwaili,MinWu,andIbrahim Alrashdi."Blockchain and fog computing in IoT-driven healthcare services for smart cities." Journal of Healthcare Engineering 2022 (2022).
7. Akhter Md Hasib, Kazi Tamzid, Ixion Chowdhury, Saadman Sakib, Mohammad Monirujjaman Khan, Nawal Alsufyani, Abdulmajeed Alsufyani, and Sami Bourouis. "Electronic health record monitoring system and data security using blockchain technology." Security and Communication Networks 2022 (2022): 1-15.
8. Namasudra,Suyel,PratimaSharma,RubenGonzalezCrespo,andVimal Shanmuganathan."Blockchain-basedmedical certificate generation and verification for IoT-based healthcare systems." IEEE Consumer Electronics Magazine (2022).
9. Azbeg,Kebira,OuailOuchetto,andSaidJaiAndaloussi."AccessControlandPrivacy-PreservingBlockchain-BasedSystem for Diseases Management." IEEE Transactions on Computational Social Systems (2022).
10. Odeh,Ammar,IsmailKeshta,andQasemAbuAl-Haija."AnalysisofBlockchainintheHealthcare Sector:Applicationand Issues." Symmetry 14, no. 9 (2022): 1760.
11. D.Bentley. TheInsidiousProblemofCounterfeitinginHealthcare. Accessed:Feb. 26,2022.[Online].
12. S. Webster. Tackling the Challenge ofCounterfeitMedicalDevices Across GlobalHealthcare Settings. Accessed: Mar. 9, 2022.
13. MedicalDevice&EquipmentFraud. Accessed:Mar. 2, 2022.[Online].
14. A.Hern. HackingRiskLeadstoRecallof500,000PacemakersDuetoPatientDeathFears. Accessed:Mar. 9,2022.
15. U.S. FoodandDrugAdministration. ClassifyYourMedicalDevice.Accessed:Sep. 12, 2022.