Blockchain-enabled secure and scalable IOT data sharing framework for Healthcare application

Chandrika G. V.[1], Venkatesh A.[2]
[1]*Selection grade lecturer E & C, Government polytechnic Mulbagal.*
[2] *Lecturer E & C, Government polytechnic, Nagamangala.*

Abstract

Improvements in patient care, the introduction of remote monitoring, and the generation of massive amounts of important healthcare data are just some of the benefits of the widespread adoption of Internet of Things (IoT) technology. The secure and scalable transfer of such information, however, remains a major obstacle. Traditional approaches to healthcare data sharing have limitations in areas such as data security, data interoperability, and data volume and diversity as a result of the Internet of Things (IoT).

This study offers a blockchain-enabled safe and scalable Internet of Things (IoT) data exchange platform for healthcare applications to overcome these issues. Blockchain technology provides a distributed and immutable ledger for exchanging data securely and efficiently while maintaining data integrity, transparency, and privacy. The framework takes advantage of blockchain's defining characteristics, such as decentralization, consensus mechanisms, and smart contracts, to build a safe and effective network for exchanging information. Several interrelated parts make up the suggested framework. Internet-of-Things devices produce real-time healthcare data since they are sensor-equipped and linked to the network. Intermediary data collectors gather, verify, and encrypt the data before sending it to the blockchain. Healthcare data is stored and managed securely through the blockchain network, which is made up of dispersed nodes. Through secure channels, data users like doctors and scientists may access the information and put it to use in a wide variety of medical fields.

The framework's data flow is controlled to guarantee safe and effective communication between its many parts. The data generated by IoT devices is continually gathered by data collectors. Data gathered is checked for errors, encrypted, and uploaded to the blockchain network using consensus procedures to maintain data honesty and openness. Secure authentication systems, smart contracts, and data sharing regulations all stored on the blockchain allow users to access the data. Patients are able to modify their data consent and privacy choices because to the framework's fine-grained control over data access. There are several advantages to incorporating blockchain technology into the architecture. To begin, the immutability and distributed nature of the blockchain safeguards information from corruption. Second, using consensus methods improves data security and reliability by requiring consensus from a majority of nodes before a data transaction can be completed. Smart contracts, thirdly, automate data sharing policies, making all data transactions visible and auditable. Blockchain's scalability also ensures that this architecture can accommodate the growing quantity and variety of healthcare data produced by IoT devices. However, the suggested framework confronts many obstacles in its actualization. Major obstacles that must be overcome include managing data ownership and consent, ensuring interoperability with existing healthcare systems, resolving regulatory compliance, and developing trust among stakeholders. More and more healthcare data and Internet of Things devices mean that scalability and performance optimization are must-haves.

Keywords- Blockchain technology, Internet of Things (IoT), Healthcare data sharing, Secure data sharing, Scalable data sharing, Data integrity, Data privacy, Interoperability, Consensus mechanisms, Smart contracts

DOI : 10.21904/weken/2022/v7/i2/173014

I. INTRODUCTION

The healthcare industry is just one that has benefited greatly from the advancements made possible by the Internet of Things (IoT) in recent years. Possibilities for enhancing patient care, streamlining operations, and advancing medical research have expanded because to the availability of real-time data collected and analyzed through linked devices. However, several obstacles have emerged as a result of the broad use of IoT in healthcare, especially in regards to safe and scalable data exchange. Because of the importance of healthcare data confidentiality, interoperability, and privacy, new approaches are needed to successfully handle these issues.

When it comes to IoT data, the traditional means of exchanging information in healthcare, such as centralized databases and file transfer protocols, have considerable limits. Data storage, processing, and sharing become difficulties when the volume and speed of data created by IoT devices overwhelm existing infrastructures. Integrity and privacy issues are exacerbated by the fact that centralized systems have just one possible point of failure. The lack of a safe and scalable infrastructure for exchanging IoT data in healthcare applications is highlighted by these constraints.

Blockchain technology has shown great promise as a way to safely and flexibly share information. Blockchain is a distributed ledger technology that was initially designed for digital currencies like Bitcoin. It provides a decentralized and tamper-proof platform for storing and managing data. Blockchain uses cryptography and consensus methods to ensure that all parties can see and trust the same information. Due to its immutability, decentralized nature, and ability to scale, blockchain is well-suited to the development of a healthcare IoT data sharing platform.

By bringing together the benefits of IoT devices, blockchain technology, and smart contracts, the suggested architecture for blockchain-enabled safe and scalable IoT data sharing in healthcare applications creates a powerful ecosystem. Internet of Things (IoT) devices or sensors, data collectors, a blockchain network, and data consumers including healthcare practitioners, researchers, and patients are all parts of the architecture. Together, these parts guarantee the confidentiality, integrity, and availability of sent data (Novo & Oscar, 2018).

The system relies heavily on Internet of Things (IoT) devices to collect data in real time from patients, medical equipment, and other sources. The information is gathered by the data collectors, who then encrypt and upload the data to the blockchain. The data is maintained in a distributed and unchangeable ledger called the blockchain network, which consists of a collection of interconnected nodes (Atlam, Alenezi, Alassafi, Wills, & Gary, 2018). Data suppliers and users can benefit from smart contracts, which are self-executing programs stored on the blockchain and used to enforce predetermined rules and automate transactions. Data sharing agreements, access restrictions, and regulatory compliance may all be managed with the use of these contracts.

Integrating blockchain technology into healthcare data exchange has several benefits, one of which is increased security and privacy. The confidentiality, integrity, and availability of patient health records are of the utmost importance and must be safeguarded at all costs. The cryptographic techniques and distributed ledger design of blockchains offer strong protection against such threats. Furthermore, the framework uses encryption methods to protect data during transmission and storage, restricting access to those who should have it. The framework allows healthcare companies to develop and enforce data sharing rules based on the individual needs and permissions of each participant by constructing a permissioned blockchain network with granular access control (Rajput, Li, Ahvanooey, & Milad, 2021).

DOI : 10.21904/weken/2022/v7/i2/173014

The suggested approach also takes into account the important issue of scalability. The sheer volume of data produced by IoT devices threatens to swamp current methods of information exchange. The framework utilizes many techniques, including off-chain storage solutions and layer 2 protocols, to guarantee scalability. The concept of "off-chain storage" refers to the practice of keeping data outside of the blockchain but yet ensuring its security through cryptographic hashes. State channels and sidechains are examples of Layer 2 protocols that may be used to execute a large number of transactions independently from the main blockchain (Wu, et al., 2019).

A. Overview of the importance of IoT data sharing in healthcare

Patient care, operational efficiency, and medical research have all been profoundly impacted by IoT's introduction into the healthcare sector. Wearable sensors, medical monitoring devices, and smart healthcare equipment are all examples of Internet of Things (IoT) gadgets that produce massive volumes of real-time data with great potential for enhancing healthcare results. Only until information is effectively shared between healthcare professionals, researchers, and patients will the full benefits of IoT in healthcare be realized. Sharing data through the Internet of Things (IoT) has enormous potential to improve healthcare in many ways (Rayan, Rehab, Tsagkaris, Christos, Romash, & Iryna, 2021).

Better patient care is one of the main benefits of data sharing in the IoT. The Internet of Things (IoT) has made it possible for healthcare practitioners to remotely monitor patients, identify early warning indications, and take immediate action. For people with long-term health issues like diabetes or cardiovascular disease, for instance, wearable gadgets can help doctors keep tabs on things like heart rate, blood pressure, and glucose levels. By pooling their resources, healthcare providers may gain a more complete picture of each patient's condition and respond more effectively and efficiently. Patient outcomes, hospital readmission rates, and quality of life are all improved by this preventative method of care.

The exchange of data through the Internet of Things also improves healthcare companies' productivity. Healthcare providers may improve efficiency, effectiveness, and satisfaction with patient care by implementing IoT devices and exchanging data across systems and divisions. For instance, IoT-enabled medical devices may provide real-time data to EHR systems, which can then automate data entry and get rid of human error. This streamlined sharing of information boosts productivity, lessens the burden of paperwork, and frees up medical personnel to devote more time to caring for patients. Predictive analytics and machine learning algorithms may then be applied to this pooled data to provide insights that improve scheduling, inventory management, and resource usage.

Sharing data from IoT devices might have a profound impact on medical science. IoT data may help research institutes perform large-scale investigations, learn more about illness trends, and discover cures more quickly. Institutional collaboration, validation of findings, and generation of comprehensive datasets are all facilitated by the safe transfer of anonymised and aggregated IoT data. Innovation is encouraged, study repeatability is enhanced, and the application of research results to clinical practice is accelerated by this method of collaborative research. By revealing health patterns, foreseeing disease outbreaks, and guiding public health policies, the exchange of IoT data can also aid in population health management.

Patient autonomy and active participation are also essential components of healthcare IoT data exchange. Giving patients access to their own Internet of Things (IoT) health data empowers them to take an active role in their care. By keeping tabs on their vital signs, patients may see how they're doing in terms of reaching their own health objectives and learning how their decisions affect their overall health.

DOI : 10.21904/weken/2022/v7/i2/173014

Because of this openness and participation, people are better able to manage their health, make educated decisions, and work closely with their healthcare teams. In addition, patients can provide healthcare providers with data they produce themselves, opening the door to telehealth, telemonitoring, and other virtual care options. Care coordination is improved, healthcare expenses are decreased, and patient satisfaction is raised with this patient-centric strategy.

Despite many benefits, there are also some special difficulties associated with exchanging IoT data in healthcare. Because of the personal nature of the information included in healthcare records, certain privacy and security safeguards are required. Secure authentication, encryption, and access restrictions are essential for IoT data exchange frameworks to prevent data breaches and illegal access. In addition, data governance frameworks and interoperability standards are crucial for facilitating communication and information sharing among all the parties involved in healthcare.

B. Challenges and limitations of existing data sharing methods

In healthcare, where efficient information interchange is essential for providing high-quality treatment to patients, conducting research, and improving healthcare operations, data sharing plays a particularly important role. However, conventional approaches of coordinating and utilizing healthcare data are typically plagued with difficulties and restrictions. Recognizing the importance of novel approaches, such as blockchain-enabled frameworks, to overcoming these constraints requires an appreciation of the difficulties that must first be surmounted. Let's have a look at some of the major obstacles and restrictions of today's healthcare data sharing practices.

Lack of interoperability between systems and platforms is a major barrier to the free flow of healthcare data. Many healthcare organizations struggle with data interchange and integration due to the usage of incompatible electronic health record (EHR) systems, data repositories, and data formats. Fragmented patient records, data duplication, and restricted data accessibility result from the absence of standards, which hinders effective data exchange and collaboration across healthcare providers.

Healthcare data is generally kept in several systems, leading to data fragmentation and dispersion over a variety of databases. This dispersion makes it difficult to consolidate and harmonize data from many sources, leading to inaccurate and insufficient patient profiles. Researchers have a hard time getting a complete picture of patient health or studying populations as a whole due to the fragmented nature of the data they have access to (Goble, Carole, Stevens, & Robert, 2008).

Protecting the privacy and security of patients' medical records, unique identifiers, and genetic information is a top priority in the healthcare industry. Concerns about data security and patient privacy are paramount while collaborating in the healthcare industry. Many of the current approaches to data sharing rely on centralized infrastructures that can be easily compromised. The need for strong encryption, access restrictions, and data anonymization mechanisms increases when data is transferred between several businesses or groups.

Management of data sharing agreements and patient consents is a crucial aspect of healthcare that requires careful attention to governance. Lack of defined techniques for gaining patient consent and maintaining data access permissions is a common problem with current approaches. When numerous companies are involved in data sharing, the already complicated task of managing permission becomes even more so. Concerns about ethics and legality, as well as setbacks to data-sharing efforts, might result from inadequate consent management.

Existing data sharing mechanisms are unable to keep up with the growing volume, velocity, and diversity of data due to the proliferation of IoT devices and the exponential increase of healthcare data.

DOI : 10.21904/weken/2022/v7/i2/173014

When dealing with enormous datasets, traditional systems may encounter performance difficulties, storage restrictions, and transmission delays. As the need for data exchange increases, it becomes increasingly difficult to scale up current infrastructure to meet it.

Maintaining the honesty and reliability of shared data is essential in the healthcare industry. Existing methods of exchanging information frequently lack procedures to ensure that the information being communicated is correct, legitimate, and immutable. Patient safety, research results, and data integrity can all be jeopardized by data manipulation, tampering, or illegal changes.

Privacy and security legislation, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union, place stringent requirements on the sharing of healthcare data. There may be legal and regulatory hurdles if current data exchange mechanisms are unable to conform to these standards. When data is shared across borders or involves numerous governments, ensuring compliance becomes much more complicated.

C. Introduction to blockchain technology and its potential for secure and scalable data sharing

While blockchain technology was initially developed to power cryptocurrencies like Bitcoin, it has now expanded into a flexible solution with potential uses in many other fields. Blockchain is ideally suited for secure and scalable data exchange because to its decentralized structure, transparency, and rigorous security features. The healthcare industry is one of the most recent to embrace blockchain technology due to the industry's pressing need for safe, interoperable, and private data exchange. This article introduces blockchain technology and discusses its potential to transform healthcare information exchange.

In its most basic form, a blockchain is a distributed ledger that keeps track of data or transactions over a network of computers. Transactions are added to the ledger in a sequential and immutable fashion, and each node keeps a copy of the ledger. Because all nodes must agree to make any changes to the distributed ledger, the data in it can be trusted to be accurate and complete. In addition, blockchain uses cryptographic methods to safeguard information, making it impossible to modify records without being noticed.

Blockchain's decentralized nature is a major selling point. Blockchain facilitates decentralized data exchange between users, as opposed to the centralized data control of traditional centralized systems. This distributed design reduces the need for a governing body, which in turn decreases reliance on middlemen and increases data openness. This decentralized method has the potential to greatly improve the flow of health information among patients, doctors, researchers, and other interested parties.

The issue of secure data storage is another one that blockchain technology can solve. Data recorded on a blockchain is encrypted using cryptographic techniques to prevent unauthorized parties from accessing it. The distributed ledger design of the blockchain also makes it exceedingly resistant to manipulation and attack. It is extremely difficult for an attacker to undermine the integrity of data kept on a blockchain since doing so would require them to obtain control of the majority of the network's computational power.

In addition, blockchain technology allows for the verification of the veracity of exchanged data and the establishment of trust between parties. The blockchain records every transaction with a timestamp and a cryptographically secure hash, making it possible to track the data back to its original source and examine its entire history. This openness fosters confidence since any participant may check the veracity of the data without consulting a third party.

DOI : 10.21904/weken/2022/v7/i2/173014

This has the potential to have far-reaching effects on healthcare systems, including data quality, clinical research, and the management of medicinal supply chains.

Blockchain technology also shows promise in terms of scalability. When it comes to massive amounts of data or a high rate of transactions, traditional data sharing solutions typically fall short. These scalability issues may be addressed with the help of blockchain technology. Off-chain processing, in which certain transactions are processed outside of the main blockchain, and sharding, in which the blockchain is divided into smaller pieces, are two methods that can dramatically enhance scalability while retaining data integrity and security (Kim, Soohyeong, Kwon, Yongseok, Cho, & Sunghyun, 2018).

Blockchain technology has vast promise in the healthcare industry, especially for facilitating the safe and scalable exchange of patient information. By allowing for secure and transparent data transfers between healthcare providers, blockchain technology can improve the quality and timeliness of patient treatment. This has the potential to boost care coordination, cut down on mistakes in the healthcare system, and boost patient outcomes. Researchers may gain access to massive datasets without compromising the privacy of their subjects by using blockchain technology to provide safe and private data sharing.

In addition, healthcare supply chains may be made more transparent and efficient with the use of blockchain technology. Pharmaceuticals, medical equipment, and other healthcare items may be tracked and verified on the blockchain, which helps fight counterfeit medications, guarantees product quality, and increases patient safety.

II. BACKGROUND

Technological improvements and the demand for more efficient and effective healthcare delivery have prompted a digital revolution in the healthcare business. This shift has been largely fueled by the advent of IoT, which has opened up new avenues for collecting, monitoring, and analyzing data in real time from networked medical equipment. Wearable sensors, medical gadgets, and smart healthcare equipment are all examples of Internet of Things (IoT) products with the potential to transform patient care, boost operational efficiency, and pave the way for ground-breaking medical discovery.

As more and more healthcare facilities use IoT solutions, huge volumes of data are being produced. This information may be used to better serve patients, enhance healthcare delivery, and expand our understanding of the human body. However, a strong and secure data exchange infrastructure that guarantees interoperability, privacy, and scalability is essential for extracting the full potential of IoT data.

In healthcare, the unique properties of IoT data provide substantial hurdles for traditional data exchange mechanisms like centralized databases and file transfer protocols. The huge amount, velocity, and diversity of data created by IoT devices is beyond the capabilities of these technologies. Data security, privacy breaches, and single points of failure are all things to think about when it comes to these centralized systems. As a result, a safe and privacy-preserving data exchange solution is essential given the sensitivity of healthcare data and the stringency of regulatory regulations governing its use.

The need for safe and scalable healthcare data sharing has led many to look to blockchain technology as a possible answer. Blockchain is a distributed ledger system that was initially created as the underpinning technology for crypto currencies like Bitcoin. It provides a decentralized and tamper-proof platform for storing and managing data. Blockchain's openness, immutability, and cryptographic security are all perfect for the healthcare industry, where IoT data must be shared in a safe and scalable manner.

DOI : 10.21904/weken/2022/v7/i2/173014

When it comes to exchanging medical records, blockchain technology has numerous significant benefits. For starters, it's distributed nature makes a governing body superfluous, allowing for data to be exchanged directly between users. The data exchange procedure is simplified because of this decentralization, which also increases data transparency and decreases the need for middlemen. Second, once data is stored on the blockchain, it cannot be changed, guaranteeing data integrity and auditability. This is especially crucial in the healthcare industry, where maintaining the privacy and security of patient information is a top priority. Finally, the blockchain's use of cryptographic methods makes it an excellent tool for safeguarding private medical information. The blockchain encrypts all data and restricts access to it to only those who have been granted permission to view it. Finally, smart contracts, which are programmable self-executing contracts implemented on the blockchain, make it possible to automate data sharing agreements, access controls, and regulatory compliance. By allowing parties to set and enforce their own rules, smart contracts make it possible to exchange data in a safe and manageable way.

Blockchain-enabled safe and scalable IoT data exchange has enormous promise in the healthcare industry. Blockchain technology has the potential to revolutionize the efficient exchange of medical records. Blockchain technology allows healthcare practitioners to safely share and access accurate patient records independent of their location or the electronic health record system (EHR) in use. Care coordination is enhanced, medical mistakes are reduced, and patient outcomes are enhanced as a result of this real-time data interchange. Data sharing for medical research may be made more safe and private with the use of blockchain technology. Data collected via the Internet of Things (IoT) may be accessed and analyzed by researchers in a safe environment, leading to discoveries that can expand medical understanding and enhance treatment regimens.

Additionally, blockchain technology can enhance healthcare businesses' operational efficiency. Blockchain enables secure and transparent supply chain management, which in turn allows for the tracking and verification of the validity of healthcare items including medications, medical equipment, and more. Patient safety is improved, medicine counterfeiting is prevented, and product quality is guaranteed.

However, it's crucial to note that there are obstacles to overcome when establishing a blockchain-enabled safe and scalable IoT data exchange framework in healthcare. The first major obstacle is the lack of standardization among IoT devices and platforms. The integration and interchange of data between various devices and systems relies on the success of standardization initiatives. Second, it is essential to protect user privacy and follow all applicable laws and standards. Blockchain solutions for the healthcare industry must respect patient privacy and consent in accordance with applicable laws and regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in Europe. Third, scalability is important because the blockchain has to be able to process the enormous amount of data produced by IoT devices without slowing down. Finally, in order to ensure a smooth transition, it is essential to carefully design and implement the integration of blockchain technology into the existing healthcare infrastructure.

A. Explanation of IoT devices in healthcare and their data generation capabilities

The healthcare industry is no exception to the widespread changes brought about by the Internet of Things (IoT). Internet of Things (IoT) devices in healthcare include sensors and other gadgets that track and report information about patients, medical equipment, and healthcare facilities. The real-time data collecting, remote monitoring of patients, and smart decisions made possible by these gadgets have the potential to revolutionize healthcare. In this breakdown, we'll have a look at the many categories of healthcare IoT devices and the information they may collect.

DOI : 10.21904/weken/2022/v7/i2/173014

Wearable sensors are among the most well-known and commonly deployed Internet of Things (IoT) technologies in the medical field. Individuals can use these gadgets to track their heart rate, blood pressure, temperature, oxygen saturation, and activity levels in real time. Smartwatches, fitness bands, patches, and garments with built-in sensors are all examples of wearable sensors. They let people to monitor their personal well-being and health and allow medical professionals to remotely monitor patients by providing crucial real-time data on health status, activity levels, and sleep patterns.

Internet of Things (IoT) devices known as "remote monitoring devices" are used to keep tabs on patients' well-being even when they aren't at a hospital or clinic. Glucose levels for diabetic management, respiratory parameters for asthma or COPD monitoring, and heart activity for patients with cardiovascular disorders are just a few examples of the kind of information that these devices are built to gather and communicate. By allowing doctors to keep tabs on their patients' vital signs remotely, remotely monitored patients have better results and require fewer hospitalizations.

Physiological functions can be monitored and controlled by implantable medical devices, which are Internet of Things (IoT) devices that are surgically placed within the body. Pacemakers, defibrillators, neurostimulators, and insulin pumps are only few examples of implanted medical technology. These gadgets monitor vital signs including heart rate, blood sugar, and brain activity continually, and respond with treatment or notify medical staff to any irregularities. The ability to provide individualized and precise treatment for patients with chronic illnesses is made possible by implantable medical devices (Denning, et al., 2010).

Infusion pumps, blood pressure monitors, ventilators, and nebulizers are all examples of "smart medical devices" that have been updated to include Internet of Things functionality. These gadgets have sensors, network capabilities, and data processing power to gather and transmit information in real time. Smart medical devices have the potential to improve healthcare by providing precise measurements, automating data collection, and allowing for remote monitoring and control by medical professionals. These tools boost the effectiveness of medical treatments, protect patients from harm, and easily share data with EHR systems.

Sensors placed throughout healthcare facilities to track environmental factors, equipment efficiency, and patient well-being are further examples of IoT devices used in healthcare. Temperature, humidity, air quality, and even human presence may all be monitored with the help of these sensors. Healthcare facilities can maintain a safe and comfortable atmosphere for their patients, avoid costly equipment breakdowns, and identify possible threats by constantly monitoring their surroundings. These sensors aid in more effective resource management and provide a more secure and relaxing setting for hospital patients.

When it comes to healthcare, the data collected by IoT devices is both extensive and diverse. Data is being collected in real time at extremely high rates by these devices. There are many classifications that may be applied to the produced data:

Vital Signs: Heart rate, blood pressure, and respiration rate are all examples of physiological data that may be collected by an IoT device. Other examples include temperature, oxygen saturation, glucose levels, and electrocardiogram (ECG) measurements. Having access to this information allows for the prompt monitoring of chronic illnesses, the identification of abnormalities, and the facilitation of treatments.

Information Collected From Movement and Activity Trackers and Sensors These devices record information about a person's activity, such as their step count, distance traveled, sleep habits, and energy consumption. This data may be used to keep tabs on exercise, spread messages of health, and deal with problems that call for a change in routine.

DOI : 10.21904/weken/2022/v7/i2/173014

Temperature, humidity, air quality, and noise levels are just some of the environmental parameters that environmental sensors track. These statistics are essential for stopping the spread of disease and making sure everyone in the hospital has the best possible experience.

Medication Adherence Information Internet of Things devices may log when drugs are taken and remind patients to take them. This information is useful for determining a patient's level of compliance with treatment recommendations.

Images, videos, and audio recordings from diagnostic instruments like ultrasound machines and imaging devices that have been connected with the Internet of Things may be captured and sent. In cases when access to specialist healthcare practitioners is limited, this paves the way for remote consultation, expert views, and rapid diagnosis.

Integration of IoT devices and the data they provide has enormous potential to advance healthcare delivery, research, and efficiency. However, to solve the issues associated with IoT data sharing, such as data privacy, security, interoperability, and scalability, it is essential to establish safe and scalable data sharing frameworks, such as blockchain-enabled solutions.

B. Overview of the existing healthcare data sharing frameworks and their limitations

Collaboration, research, and enhanced patient care are all made possible by healthcare data exchange, making it an essential component of modern healthcare delivery. Several frameworks and technologies have been created throughout the years to make it easier to share healthcare data. Limitations of current healthcare data sharing systems are discussed in this review.

EHRs, or electronic health records, are utilized extensively by the healthcare industry for the purpose of storing and managing patients' health records. Medical professionals are able to access and exchange patient records using these platforms. However, interoperability is still a significant obstacle. Data sharing between healthcare organizations or systems is complicated by the fact that various EHR systems frequently employ different standards and formats. When sensitive patient information is shared across several parties, privacy and security concerns naturally emerge.

Exchanges enabling the secure, centralized exchange of patient health records between healthcare providers are known as health information exchanges (HIEs). HIEs are an attempt to solve the interoperability problems by mediating between different systems. Inconsistent involvement from healthcare organizations, incompatible technology, and the necessity for standardized data all work against HIEs' efficiency. Data sharing through a centralized institution also raises questions of privacy and permission.

Data Sharing in a Federated Environment Multiple healthcare organizations can pool their data resources and exchange information using a federated data sharing paradigm. Data inquiries and aggregation across various businesses are made easier in this architecture by a central coordinating entity that eliminates the need to physically move the data. Federated data sharing needs complicated technological infrastructure and data governance standards, but it alleviates privacy issues by storing data locally. It can be difficult to coordinate access to data and maintain data integrity across businesses.

When it comes to storing and exchanging information, cloud computing provides a scalable and adaptable architecture. Cloud computing allows healthcare businesses to securely store their data and make it available to approved users. While cloud-based data sharing improves accessibility and cooperation, it also raises questions of privacy, security, and regulatory compliance. Protecting sensitive information from breaches or unauthorized access is paramount when dealing with healthcare data, which is why stringent restrictions are in place.

DOI : 10.21904/weken/2022/v7/i2/173014

Data Sharing Agreements (DSAs) are legally binding contracts between healthcare institutions that spell out the parameters for exchanging information. A data sharing agreement's objective, data access rules, data ownership, and data usage limits are all spelled out in detail. Despite their usefulness as a foundation for information transmission, data sharing agreements are rarely pre-drafted and can take some effort to negotiate. And it's not easy to keep tabs on how information is being used or ensure that parties to data sharing agreements are actually doing so.

Several barriers to healthcare data exchange still exist, despite the existence of these frameworks.

Because of the wide variety of data formats, coding methods, and communication protocols used by healthcare systems and devices, interoperability remains a significant barrier. Because of this diversity, it is difficult for healthcare institutions and systems to share and integrate their data with one another.

Security and confidentiality of patient health records are of paramount importance. Safeguards against data breaches and illegal access to patient data must be built into any data sharing structure. Adding further complication is the need to comply with regulations like HIPAA and GDPR.

Data ownership determination, patient permission gathering, and data governance protocol management are all challenging aspects of healthcare data sharing. Having well-defined policies and governance frameworks in place is essential for ensuring the correct application of data and the protection of patient privacy and consent.

Because of the exponential growth of data created by Internet of Things (IoT) devices and other cutting-edge technology, traditional data exchange techniques are sometimes overwhelmed. When processing and analyzing data from real-time data sources, scalability becomes critical.

Concerns about data ownership, competitiveness, and divergent agendas make it difficult to establish trust and encourage collaboration across healthcare institutions in order to share data. Overcoming institutional hurdles and aligning incentives are necessary to build a culture of data sharing and collaboration.

C. Introduction to blockchain technology and its key features relevant to healthcare data sharing

Emerging as a game-changing invention, blockchain technology has the potential to disrupt several sectors, including healthcare. While blockchain was first developed to support digital currencies like Bitcoin, it has now expanded to become a robust platform for decentralized and encrypted information management and trade. When used to the exchange of healthcare data, blockchain's distinctive properties help meet the difficulties of confidentiality, availability, portability, and scalability. In this introductory section, we will cover the basics of blockchain technology and focus on the aspects most important to the exchange of medical records.

A blockchain is essentially a shared digital ledger that can be accessed by all members of a network and used to record and verify transactions or data. A blockchain is a distributed ledger in which each member in the network has a copy of the whole database and no one entity owns the data. Because of its decentralized structure, it guarantees transparency, immutability, and durability, making it an excellent choice for the safe exchange of medical records.

Blockchain's openness is one of its most appealing qualities. All nodes in the network will be able to view each transaction or data entry that is added to the blockchain. This openness improves confidence among stakeholders by making data-sharing operations more easily auditable and less susceptible to tampering. Transparency in the healthcare sector improves teamwork and decision-making by giving providers, researchers, and patients equal access to high-quality data.

DOI : 10.21904/weken/2022/v7/i2/173014

Blockchain technology's immutability is another essential aspect. Addition to the blockchain makes it nearly hard to change or remove a transaction or piece of data. By preventing unauthorized changes and maintaining a consistent state of stored information, immutability establishes a foundation of trust and reliability. The immutability of blockchain can aid in preventing mistakes, fraud, and illegal access in healthcare data exchange, where accuracy and consistency of patient information are of the utmost importance.

Through its use of cryptographic methods, blockchain technology also delivers high levels of safety. A blockchain is a distributed ledger that stores encrypted data and links it to the history of transactions in a series of blocks. This cryptographic protection guarantees the privacy of the data and restricts access to those who have been given the decryption keys. Blockchain's cryptographic security mechanisms aid the healthcare industry in protecting sensitive patient health information and staying in line with data protection standards.

The decentralized nature of the blockchain is another important characteristic when it comes to the exchange of healthcare data. There is no central hub or point of failure in a blockchain network. There are no middlemen or governing bodies since everyone in the network has their own copy of the ledger. This decentralization increases data availability and robustness, encourages peer-to-peer data exchange, and lessens reliance on a central authority. In healthcare, where data is spread across many different systems and organizations, a decentralized blockchain architecture allows for the safe and efficient transfer of patient information.

Blockchain technology's possibilities for healthcare data exchange are further bolstered by smart contracts, which are programmable, self-executing contracts that are placed on the blockchain. Rules, agreements, and permissions may all be programmed into a smart contract and automatically enforced. Agreements on data sharing, data access, and consent management may all be made easier using smart contracts in the healthcare industry. These programmable contracts encourage accountability and openness between parties by requiring that data exchange follow a set of standards.

Blockchain technology's defining characteristics—transparency, immutability, cryptographic security, decentralization, and smart contracts—form a solid basis for overcoming the obstacles associated with healthcare data exchange. Blockchain-based solutions take use of these qualities to provide safe, private, and scalable infrastructures for sharing medical records. Healthcare providers, researchers, and patients may all benefit from these frameworks' capacity to simplify interoperability, improve data integrity, safeguard patient privacy, and encourage teamwork.

III. ARCHITECTURAL DESIGN

Integrity, privacy, and interoperability of healthcare data rely heavily on the structural design of a blockchain-enabled safe and scalable IoT data exchange framework in healthcare. This architecture includes all the parts, protocols, and interactions required to make it possible for IoT devices, healthcare providers, and other parties to share data without any hitches. The essential components of such a framework will be outlined below.

The Internet of Things (IoT) device layer is the architecture's groundwork, consisting of a wide variety of sensors and other devices linked together by networking. Some examples of these gadgets are environmental sensors, implanted medical devices, remote monitoring equipment, and smart medical devices. Data on patient health, medical parameters, and environmental variables are all the responsibility of each IoT device. Connectivity and security features built into these gadgets are essential for protecting the reliability of the data they produce.

DOI : 10.21904/weken/2022/v7/i2/173014

Before information gathered by Internet of Things (IoT) devices can be shared on a blockchain, it must be collected, processed, and authenticated. Data collecting protocols, data aggregation methods, and data validation frameworks are all part of this layer. In order to reduce the amount of data transported to the blockchain network, it may also contain edge computing capabilities to carry out initial data processing and filtering at the device level. Data compression and encryption are two preprocessing techniques that may be used to improve data transmission efficiency and safeguard private data.

A decentralized and secure ledger for storing and managing healthcare data, the blockchain network is at the heart of the data sharing system. Each node in the network stores its own, identical copy of the blockchain. When deciding on a blockchain platform, features like scalability, consensus process, and smart contract functionality are all important considerations. Public blockchains like Ethereum and private/permissioned blockchains like Hyperledger Fabric are two of the most well-known alternatives. The blockchain network guarantees the immutability, transparency, and integrity of the distributed data, safeguarding it against hacking and other forms of interference.

To automate and enforce previously agreed upon norms and conditions for data exchange, smart contracts play a crucial role. Data access restrictions, permission management, and data sharing agreements are just some of the many uses for these self-executing contracts once they have been installed on the blockchain network. Data exchange is governed by predetermined rules and permissions thanks to smart contracts. A patient may decide who has access to their health information and under what conditions using a smart contract.

Safe data storage and encryption are essential for meeting the requirements of data protection laws and ensuring the privacy of patients whose medical records are maintained on the blockchain. To ensure the privacy of sensitive data, the design should include means for encrypted storage. To protect information while it is stored, you can use encryption methods like symmetric or asymmetric encryption. The danger of data loss or single points of failure may be minimized by using distributed storage solutions, which the design should take into account to improve data availability and resilience.

When it comes to healthcare, interoperability is essential since it allows for the smooth incorporation and interchange of data between various healthcare organizations, systems, and stakeholders. Standardized interfaces, such as HL7 FHIR (Fast Healthcare Interoperability Resources), should be incorporated into the architectural design to provide smooth data exchange. Secure and consistent data communication between the blockchain network and existing healthcare systems is made possible via the use of APIs (Application Programming Interfaces) and data exchange protocols.

Identity and Access Management: A solid identity and access management system is crucial for protecting the veracity and privacy of blockchain-stored information. The means for authenticating users and allocating privileges in accordance with established policies are provided by this layer. Trusted identities can be established with the help of public key infrastructure (PKI) and digital certificates, while data access can be managed with the help of ACLs and RBAC. Incorporating patient permission processes into identity management platforms gives patients more say over how their information is distributed (Mohammed & Ishaq Azhar, 2021).

With the use of analytics and insights capabilities, useful information may be gleaned from the pooled healthcare data. Patterns, trends, and correlations in the data may be uncovered with the use of analytics tools by employing machine learning algorithms and data mining techniques. This can be useful for tracking diseases, keeping tabs on populations, guiding doctors in making tough decisions, and furthering scientific inquiry. The approach improves the shared data's value and usability by delivering actionable insights.

DOI : 10.21904/weken/2022/v7/i2/173014

The architectural design should think about user-friendly interfaces and applications that facilitate productive stakeholder engagement with the system. This includes mobile apps, visualization tools, and dashboards that are easy on the eyes. Users should be able to examine their consent settings, track data sharing actions, and get warnings and notifications all through the interfaces. Usability and user uptake may be maximized by adhering to principles of user-centered design.

A. High-level architecture of the proposed framework

Data integrity, privacy, interoperability, and scalability are all issues that will be addressed by the proposed blockchain-enabled safe and scalable IoT data exchange framework in healthcare. Blockchain technology is used to build a trustworthy, distributed network for exchanging data in the healthcare industry. The high-level architecture is made up of the following parts:

Internet of Things Devices: The foundation is built on a wide variety of IoT devices, such as sensors used in wearables, medical equipment, and even environmental monitoring equipment. These gadgets produce information on patients' health, medical parameters, and surrounding conditions in real time. To prevent any third party from intercepting sensitive information while it is in transit, IoT devices use secure communication protocols and data encryption methods.

The information gathered by IoT gadgets is processed and verified here before it is added to the blockchain. It is possible to reduce the amount of data supplied to the blockchain network by employing data aggregation techniques and edge computing capabilities to filter and preprocess the data. Data consistency and outlier detection are only two examples of the types of errors that may be caught and corrected by data validation techniques.

The blockchain network, a distributed and secure ledger for storing and managing healthcare data, lies at the heart of the system. Multiple nodes in this network store an immutable and transparent copy of the blockchain. Scalability needs and preferred consensus processes can guide the decision between a public and private/permissioned blockchain network. By design, the blockchain network prevents tampering and protects the authenticity of every sent data.

Data Access Control and Smart Contracts: Smart contracts are computer programs that may be placed on a blockchain to automate and enforce certain criteria and regulations for the distribution of data. Data sharing agreements, permission management, and other fine-grained restrictions are all made possible through the use of contracts. Data exchange is governed by predetermined rules and permissions thanks to smart contracts. For instance, a smart contract might mandate certain levels of patient consent and limit access to certain doctors and researchers.

Secure data storage and encryption are essential for the privacy of patients whose medical records are stored and exchanged on the blockchain. Strong data encryption methods are built into the design, keeping private data just that. Together, encrypted storage techniques and distributed storage systems improve data availability, resilience, and security against manipulation and intrusion.

The Interoperability Layer provides the foundation for sharing information effectively across the many players in the healthcare industry. In order to promote interoperability, the design makes use of standard-based interfaces like HL7 FHIR. Secure and consistent data communication between the blockchain network and existing healthcare systems is made possible via the use of application programming interfaces (APIs) and data exchange protocols. This facilitates interoperability and integration, leading to better healthcare data exchange.

Identity and Access Management: A strong identity and access management system is established to guarantee the originality and accuracy of all data stored and sent over the blockchain.

DOI : 10.21904/weken/2022/v7/i2/173014

The means for authenticating users and allocating privileges in accordance with established policies are provided by this layer. Access control techniques manage data access based on role-based permissions and patient consent, while public key infrastructure (PKI) and digital certificates provide trustworthy identities.

In order to extract useful information from the pooled healthcare data, the architecture combines analytics and insights capabilities. Machine learning algorithms and data mining are two examples of advanced analytics tools and approaches that may be used to find patterns, trends, and correlations in data. These discoveries improve the value and usability of the shared data by aiding in disease surveillance, population health management, clinical decision support, and medical research.

Stakeholders can easily interact with the system through user interfaces and apps. Effective stakeholder interaction with the framework is enabled via user-friendly dashboards, visualization tools, and mobile applications. Users may access their consent settings, track data sharing actions, view warnings, and more using these streamlined dashboards. Principles of user-centered design guarantee an easy and intuitive interaction.

The proposed framework's high-level architecture integrates Internet-of-Things (IoT) devices, data collection and processing, blockchain networks, smart contracts, data encryption, interoperability, identity management, analytics, and user interfaces to produce a safe, scalable, and private environment for sharing medical records. The framework allows for the secure and efficient sharing of healthcare data across stakeholders by combining blockchain technology and the capabilities of the Internet of Things to overcome the constraints of conventional data sharing techniques.

B. Components and their functionalities, including IoT devices, data collectors, blockchain network, and data consumers

Several crucial components work together in the proposed blockchain-enabled secure and scalable IoT data sharing architecture in healthcare to guarantee data integrity, safeguard patient privacy, and promote efficient data exchange. Internet of Things gadgets, data collectors, the blockchain infrastructure, and data users all make up these parts. Let's take a closer look at the roles played by the various parts:

Internet of Things Devices: IoT devices are crucial to the framework because they gather and generate real-time data on patient health, medical parameters, and environmental variables. Wearable sensors, medical equipment, and even environmental sensors all fall within this category. Connectivity features, such as Wi-Fi or Bluetooth, are included into IoT devices to ensure the safe transfer of data. They may also include built-in data encryption methods to keep information safe while in transit. In order to provide a steady flow of useful data for medical research, IoT devices are designed to monitor and record data in real time.

In order to prepare the data created by IoT devices for dissemination on the blockchain network, it must first be collected, aggregated, and preprocessed by data collectors. In this layer, edge computing may be used to do data processing and filtering directly on the device. In order to optimize bandwidth use on the blockchain network and reduce the amount of data supplied to the network, data aggregation techniques are used to aggregate and summarize the gathered data. Data collectors also do checks to make sure the data they've acquired is correct, consistent, and complete. Their purpose is to guarantee that only trustworthy information is distributed over the blockchain.

Blockchain Network: The blockchain network is the backbone of the whole structure, serving as a distributed and trustworthy registry for patient records. Multiple nodes store an identical copy of the blockchain, guaranteeing its immutability, integrity, and openness. Information may be shared among members in the blockchain network with complete confidence that their privacy will be protected.

DOI : 10.21904/weken/2022/v7/i2/173014

It uses cryptographic techniques to protect the privacy, integrity, and validity of stored information. The purpose of a blockchain network is to provide a secure and auditable platform for exchanging and verifying shared data, as well as to impose data access limits via smart contracts (Zheng, et al., 2017).

"Data Consumers" are the entities in the system that make use of the pooled healthcare data for things like research, analysis, treatment, and decision-making. Providers, researchers, drug makers, insurers, and government health departments are all examples. In order to access and use the shared data for their own purposes, data consumers log into the blockchain network. They may employ analytics software, ML algorithms, and data visualization methods to infer information and make wise choices. The role of data consumers is to put the pooled information to good use in areas such as patient care, scientific inquiry, and technological advancement.

Secure and scalable IoT data exchange in healthcare requires the coordinated effort of all of these parts. Data is constantly being generated and gathered by IoT devices, and then preprocessed. A blockchain network receives the preprocessed data in a safe manner and stores it in a distributed and immutable manner. Data access rules enforced by smart contracts limit access to just those who need it. Consumers of the data may use the blockchain to access, retrieve, and evaluate the pooled information, empowering them to make evidence-based decisions and promote medical progress.

C. Explanation of the data flow and interactions between different components

Data and interactions between the various parts of the proposed blockchain-enabled safe and scalable IoT data sharing architecture in healthcare are organized in a way that guarantees both security and efficiency. Let's take a closer look at the components' interactions and the data flow between them.

Internet of Things Devices: These devices are the starting point of the data flow since they are constantly gathering and producing data on patients' health, medical parameters, and surrounding environments. These gadgets collect information using a wide variety of sensors and send it on in a safe and reliable manner to the data aggregators. There may be encryption measures built into the IoT devices to keep the acquired data secure while they are transmitted from the devices to the data collectors.

Data Collectors: Data collectors are responsible for collecting information from various Internet of Things devices. The data is first aggregated and preprocessed, meaning it is consolidated and summarized before being sent to the blockchain network. As a result, system efficiency and bandwidth utilization are both enhanced. In addition, data collectors do validation checks to guarantee the truthfulness, uniformity, and completeness of the information amassed. Any discrepancies or anomalies are marked for investigation. After the data has been preprocessed and confirmed, the collectors send it to the blockchain network in a safe manner so that it may be stored and shared.

The blockchain network is the backbone of the whole infrastructure since it allows for the safe and transparent transfer of data between users. The data collectors' raw input is processed and verified before being deposited on the blockchain in a distributed and unchangeable ledger. Transactions are the means through which participants in a blockchain network exchange information with one another and with the outside world. Data privacy, integrity, and verifiability are all safeguarded by cryptographic techniques used by the blockchain network. Data access restrictions, permission management, and other requirements for data sharing may all be codified in smart contracts and then automatically enforced. Users of the shared data interact with the blockchain to access and process it for their own purposes.

DOI : 10.21904/weken/2022/v7/i2/173014

Users: Users access the blockchain network to retrieve and utilize the shared healthcare data, including healthcare practitioners, researchers, and public health authorities. They use the blockchain network to ask for and get data sets that are under their purview and retrieval criteria. Users of the data can get insights through the use of analytics software, machine learning algorithms, and data visualization methods. Improved patient care, research, and healthcare decisions are all possible thanks to the studied findings. The ecosystem benefits from a constant stream of information, made possible by data consumers adding fresh data to the blockchain network.

To guarantee a safe and effective data flow, the framework's components are coordinated with one another. The data collectors continually gather data from the IoT devices, which is subsequently preprocessed. The data is sent to the blockchain network in an encrypted form for safekeeping and distribution. Consumers of the data engage with the blockchain network to access and evaluate the pooled information, which leads to healthcare improvements. In addition, the blockchain network ensures the privacy and security of user data by enforcing restrictions over data access, consent management, and preset rules via smart contracts.

IV. BLOCKCHAIN INTEGRATION

The inclusion of blockchain technology is essential to the proposed architecture for safe and scalable healthcare IoT data exchange. The framework improves the four areas of concern in data sharing—integrity, privacy, security, and interoperability—by utilizing blockchain technology. Let's have a look at the most important features of the framework's blockchain integration:

One of the main benefits of blockchain technology is that it provides decentralized and immutable data storage. The suggested system makes use of the blockchain as a distributed ledger for keeping track of medical records. Every node in the network keeps their own copy of the blockchain, which increases security, reliability, and auditability. Once data is stored on the blockchain, it cannot be changed or tampered with, offering a strong method for data integrity thanks to the blockchain's immutability.

Data Access Control through Smart Contracts: A core feature of blockchain technology, smart contracts are computer-generated agreements that carry out their terms automatically based on a set of predetermined criteria and parameters. In the proposed architecture, smart contracts are used to manage permission and regulate who may access data. Health data is protected by smart contracts that outline who has access to the information and under what circumstances. If a patient wants just certain doctors or researchers to have access to their medical records, a smart contract can make that happen.

Strengthened Data Privacy and Security Healthcare applications have a special need for data privacy and security. The blockchain improves the privacy and security of transactions. To begin, cryptographic algorithms guarantee the integrity and privacy of the collective data. Encryption methods can be used to safeguard private data. Second, the blockchain network's decentralized design makes it less susceptible to cyberattacks and eliminates the possibility of a single point of failure. Data security may be improved because to the immutability and transparency of the blockchain's audit trail.

Healthcare data exchange faces a significant barrier due to a lack of interoperability between systems. Integrating interoperability standards and protocols into blockchain technology is one solution to this problem. The suggested framework allows for the use of standard-based interfaces like HL7 FHIR (Fast Healthcare Interoperability Resources) to make it possible for various healthcare systems and stakeholders to share data without any hitches. Standardized interfaces facilitate interoperability and integration, allowing for the safe and efficient transfer of data across programs and systems.

Consistency and trust in data are critical components of a trustworthy healthcare data exchange infrastructure. Blockchain technology's distributed and synced ledger across various network nodes guarantees data integrity.

DOI : 10.21904/weken/2022/v7/i2/173014

Each node in the network checks and double-checks each transaction, protecting the reliability of the data everyone uses. Blockchain's decentralized consensus method assures that everyone uses the same version of the truth, which boosts confidence in the system.

Data transfers inside the proposed framework are now visible and auditable thanks to Blockchain's incorporation. Data stored on the blockchain is immutable because each transaction includes a timestamp and a link to previous ones. Data can be easily tracked and verified thanks to this audit trail, which also encourages accountability on the part of all involved parties. Accountability is further improved by the blockchain network's transparency, which allows for the monitoring and verification of the actions of all participants.

Given the massive amount of data produced by IoT devices, scalability is a crucial aspect in healthcare data exchange. Sharding, sidechains, and off-chain solutions are some of the ways that blockchain technology has developed to deal with scalability issues. The suggested framework can enhance efficiency and increase transaction throughput with the help of these methods, allowing for effective data exchange even in massive healthcare networks.

A. Detailed explanation of how blockchain technology is integrated into the framework

The suggested architecture for healthcare IoT data exchange incorporates blockchain technology without causing any noticeable disruptions. Smart contracts, blockchain networks, encryption algorithms, and consensus processes will all be incorporated as part of the integration process. Let's dive into the specifics of the framework's use of blockchain technology:

Healthcare data is stored on a distributed and unchangeable ledger called the blockchain network, which is a crucial part of the system. Each node in the blockchain network stores its own copy of the blockchain. The lack of a central authority promotes openness, reliability, and robustness. Consensus methods like Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT) are used by the blockchain network to verify and settle on the transactions that are recorded there. By using a blockchain network, sensitive information may be safely and immutably kept.

When it comes to implementing data access control, consent management, and set rules inside the framework, smart contracts play a pivotal role. The rules and conditions of smart contracts are written into computer code, making the contract automatically executable. The regulations for accessing and sharing healthcare data are defined in the proposed framework using smart contracts. Consent preferences can be used by a smart contract to restrict access to sensitive information to just those parties who have been given permission to see it. Data sharing, data updating, and consent revocation are just some of the specified activities that may be automatically and transparently executed by smart contracts when certain circumstances are satisfied.

Integrating a blockchain solution requires the use of cryptographic methods to safeguard the privacy, security, and veracity of stored information. To ensure the confidentiality and security of patient information, cryptographic methods such asymmetric encryption, symmetric encryption, and hash functions are used. By encrypting data with a public key and decrypting it with a private key, asymmetric encryption ensures the security of communication and data exchange between parties. Data integrity and tampering may be checked by using the cryptographic hashes generated by hash functions. The exchanged information is well-protected thanks to these encryption techniques.

Encryption processes: The use of blockchain technology inside the framework allows for the incorporation of data encryption processes, further enhancing data security. To encrypt data, one must use encryption keys to convert the data from its original form into ciphertext.

DOI : 10.21904/weken/2022/v7/i2/173014

Only authorized parties have access to the decryption keys necessary to read the encrypted data. The information is safe and unreadable even if it is intercepted. Encryption provides an additional degree of security for private medical records, preventing illegal access and protecting patient confidentiality.

Agreement among network members on the authenticity of transactions and the sequence in which they are added to the blockchain is made possible by consensus mechanisms, which are essential to blockchain networks. Depending on the needs of the framework, many consensus techniques can be used. These include Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT). Only legitimate transactions are uploaded to the blockchain, and the shared data's integrity is protected, thanks to consensus procedures. These procedures foster confidence and agreement among members, doing away with the requirement for top-down regulation.

The suggested framework incorporates blockchain technology to enable safe, verifiable, and auditable data exchange in healthcare. Smart contracts enforce data access control and consent management, while the blockchain network operates as a decentralized and immutable record. Data encryption methods and cryptographic algorithms provide a new level of confidentiality. Validity and trustworthiness of shared information are protected through consensus methods. These interconnected parts make possible a solid framework for safe, scalable, and interoperable IoT data exchange in the medical field.

B. Use of distributed ledger for storing and managing healthcare data

The proposed blockchain-enabled safe and scalable IoT data sharing system relies heavily on the usage of a distributed ledger for storing and managing healthcare data. There are a number of ways in which healthcare data management might benefit from distributed ledger technologies like blockchain. Let's take a look at the pros and drawbacks of implementing a distributed ledger for medical records.

The proposed approach uses a distributed ledger to store healthcare data among numerous nodes or participants, guaranteeing decentralization and data redundancy. Because every node in the network has a copy of the ledger, there is no central authority or single point of failure. Data redundancy is improved by decentralization since numerous copies of the data are distributed throughout the network. This redundancy strengthens data durability and lessens the possibility of data corruption or loss.

Distributed ledgers, such as blockchains, offer an immutable and tamper-proof record of data transactions, ensuring the data's integrity. After information is recorded in a ledger, it becomes encrypted and appended to a series of blocks. To protect against unauthorized changes or deletions to previously recorded information, the ledger is designed to be immutable. This function ensures openness and responsibility by bolstering data integrity and providing a record of all data modifications.

A distributed ledger can make healthcare data management more transparent and auditable. Each participant may view every single transaction that has ever been recorded on the ledger. This openness improves auditability and makes it easier to comply with regulations. The ecosystem benefits from increased trust and accountability because to the ease with which healthcare companies, researchers, and regulators can verify data's provenance, ownership, and history.

While openness is key, privacy and data confidentiality are also important factors to consider when exchanging health records. Protecting patients' personal information is a top priority, and distributed ledgers can help by employing privacy-preserving measures. Patients' privacy may be protected and data can be exchanged safely with the help of methods like cryptographic encryption and anonymization. To manage data exchange and safeguard patient privacy, smart contracts may be used to build access controls and consent management procedures.

DOI : 10.21904/weken/2022/v7/i2/173014

Due to the wide variety of healthcare data storage and management systems and formats, interoperability is a significant barrier. A distributed ledger provides a uniform environment for data exchange, which improves communication and collaboration between various healthcare entities and technologies. Data in the healthcare industry may be more easily shared and transmitted across authorized parties by adopting standardized data standards and protocols, leading to more opportunities for cooperation and better patient outcomes.

The integrity and veracity of all recorded information is protected by a distributed ledger. The network uses consensus processes to verify and approve each transaction before it is posted to the ledger. The network's data integrity is protected by a validation procedure that makes sure only legitimate information is put to the ledger. By removing the requirement for a single authoritative source and giving everyone a voice in the validation process, distributed ledgers foster a more trustworthy environment.

Distributed ledgers can solve the performance and scalability problems that plague healthcare data management. The framework's transaction throughput and speed may be increased by tools like sharding, sidechains, and off-chain solutions. These methods improve the distributed ledger's capacity to process more transactions in parallel and store more data, making it a good fit for the expanding needs of the healthcare industry.

C. Smart contracts for defining data sharing policies and automating transactions

By allowing the creation of data sharing policies and the automation of transactions, smart contracts play a crucial role in the proposed blockchain-enabled safe and scalable IoT data sharing architecture for healthcare. The rules and conditions of a smart contract are encoded in the contract itself, making it a self-executing agreement. They follow a set of rules that determine when certain circumstances must be satisfied before taking any action. Let's look at how smart contracts play a role in the architecture by setting data sharing regulations and facilitating automated transactions:

To define and enforce data sharing regulations in healthcare, smart contracts offer a strong method. Smart contracts allow interested parties to negotiate terms and conditions for the exchange of healthcare information. When it comes to a patient's medical records, for instance, a smart contract can outline the parameters for when and how information can be shared with researchers and healthcare professionals. Data sharing is governed by these rules, which can be modified to meet the needs of a certain institution, a group of patients, or a regulatory body.

Smart contracts provide consent management for the secure exchange of patient health information. By executing a smart contract, patients may give their agreement and outline the circumstances under which their data may be used. The smart contract can save the user's consent choices, limiting data sharing to the specified parties and context. Smart contracts' automated nature allows for efficient and mistake-free consent management by cutting down on paperwork and human error.

Smart contracts streamline data exchange by automating transactions inside the framework, hence removing the need for middlemen. For instance, if a healthcare professional seeks access to a patient's medical records, the smart contract may immediately determine whether or not the patient has given their permission for the provider to view the records. Under the right circumstances, the smart contract can provide a safe and verifiable data transmission. This automation expedites the exchange of data and lessens the time it takes to find the information needed to make informed healthcare decisions.

By removing the requirement for a central authority, smart contracts improve data exchange in terms of both trust and transparency. Smart contracts' inbuilt rules and conditions guarantee that data exchange is open and auditable.

DOI : 10.21904/weken/2022/v7/i2/173014

Smart contracts may be verified by anybody on the network, increasing confidence among all parties. A higher degree of trust and confidence in the data sharing process is achieved because to the immutability of the blockchain, which guarantees that the conditions of the smart contract cannot be amended or manipulated.

Smart contracts ensure transparency and auditability for all parties involved in a data exchange. The blockchain keeps track of all the transactions that occur within a smart contract, providing a record that can be verified if necessary. Data transactions may be tracked with ease thanks to the audit trail, guaranteeing proper credit for any and all efforts. Accountability is improved due to the reduced possibility of mistakes, conflicts, and fraudulent actions thanks to the transparent nature of the blockchain network and the automatic execution of smart contracts.

Healthcare data exchange is made more efficient and cost-effective with the use of smart contracts. Smart contracts lessen the burden of administration by streamlining transactions and doing away with the necessity for third-party mediators. Smart contracts expedite the process of exchanging data, which in turn allows for more prompt and accurate healthcare choices. Smart contracts' automatic execution of predetermined tasks reduces the need for human involvement, which in turn lowers the error rate and boosts productivity.

D. Consensus mechanisms for ensuring the integrity and security of the data

The proposed blockchain-enabled safe and scalable IoT data sharing system for healthcare relies heavily on consensus methods to ensure the integrity of all shared data. The blockchain network's data is safe and secure thanks to these methods. Transactions are verified, consensus is reached among the network nodes, and only trustworthy information is published to the blockchain thanks to these consensus processes. Let's look at why consensus procedures are so important for keeping information safe and sound:

All transactions must be approved by the network's consensus procedures before they are added to the distributed ledger, or blockchain. When a transaction is started, it goes through a verification process in which nodes in the network check that it is legitimate. This verification guarantees the legitimacy of the transaction and its conformity to the established parameters. Consensus methods ensure that only legitimate transactions are added to the blockchain, protecting it from any fraudulent or harmful activity.

Consensus techniques allow the members in a blockchain network to reach a consensus on the state of the blockchain. These protocols guarantee that all users agree on the legality of transactions and the sequence in which they are added to the blockchain. Consensus is the process through which all nodes in the network agree on the current state of the data and reject any competing or incompatible blockchain implementations. With this pact in place, we know that the information on the blockchain can always be trusted.

Data on the blockchain is protected against manipulation and unlawful changes thanks to consensus processes. Each new transaction forms a "block" in a continuously growing list of blocks that are cryptographically bound to one another. The consensus method makes it computationally impossible and easily detectable to edit a single block without affecting succeeding blocks. The immutability of the blockchain ensures that no alterations are made to the data, making the information more reliable and secure.

Protection from Attacks: Consensus Mechanisms are Vital to the Security of the Blockchain Network. To varying degrees and against certain sorts of assaults, many consensus techniques may be relied upon due to their unique security qualities. By requiring computational work to validate transactions, Proof of Work (PoW) consensus reduces the risk of adversaries manipulating the blockchain. When a participant's stake in the network is at danger due to harmful activity, they are less likely to engage in it. This is the idea behind Proof of Stake (PoS) consensus.

DOI : 10.21904/weken/2022/v7/i2/173014

Byzantine fault tolerance is provided via a PBFT consensus, which guarantees safety even in the face of adversarial agents. These consensus processes offer strong defenses against assaults on the data's integrity.

Consensus techniques promote confidence amongst users by doing away with the necessity for a trusted third party to verify financial dealings. Instead, members in the network share the responsibility for making choices and distributing trust among themselves. Consensus techniques improve security by removing centralized points of failure or manipulation since they guarantee that no single party controls the data. This paradigm of decentralized trust increases openness and decreases reliance on a single authority.

Healthcare applications that deal with large amounts of data must give careful thought to scalability and performance. It is important for consensus systems to balance safety and scalability. The efficiency of a network may suffer if it relies on a consensus process like Proof of Work (PoW), which is both computationally intensive and time-consuming. Proof of Stake (PoS) and Practical Byzantine Fault Tolerance (PBFT) are two examples of more recent consensus algorithms that improve upon both the speed and scalability of transaction validation. These features make it possible for the blockchain network to process massive amounts of healthcare data quickly and efficiently in real time (Li, Xiao, Wu, & Weili, 2022).

V. SECURITY AND PRIVACY

The healthcare industry is in desperate need of a safe and scalable platform for exchanging data collected through the Internet of Things (IoT). Because of the importance of healthcare data and the widespread and linked nature of IoT devices, stringent precautions must be taken to ensure the data's privacy, security, and accessibility. Let's take a closer look at the framework's most crucial privacy and security features:

Health records should be encrypted as one of the first lines of defense against unauthorized access. Data encryption renders the information unintelligible to anybody save those in possession of the correct decryption keys. To protect data at rest and in transit, the framework should use robust encryption techniques. Protecting sensitive patient data with encryption adds a robust safeguard against unwanted access and data breaches.

Data privacy can only be protected by implementing stringent access control methods and identity management procedures within the framework. Implementing access restrictions at the device, user, and data levels is recommended. All users and devices connecting to the system need to be verified and granted access according to the privileges associated with their individual accounts. Safer login methods, such two-factor authentication and biometric authentication, can be used to verify the identities of its users. Public Key Infrastructure (PKI) and other identity management protocols provide for trustworthy and private identity verification.

Protecting information in transit between Internet of Things devices, data collectors, and data consumers is essential to ensuring the integrity of collected and used data. Transport Layer Security (TLS) and Secure Shell (SSH) are two examples of secure communication protocols that may be used to encrypt data in transit and create encrypted channels. Firewalls and intrusion detection systems are examples of safe network setups that may be put in place to monitor and prevent illegal network access and protect the privacy and security of data in transit.

Methods for Protecting Individual Privacy Healthcare data exchange relies heavily on methods for protecting individual privacy. Patients' privacy may be safeguarded while still allowing for data analysis and exchange by employing methods like differential privacy, homomorphic encryption, and data anonymization. To shield users' identities, differential privacy injects random data into search results, while homomorphic encryption lets users do calculations on encrypted data without needing to decode it.

DOI : 10.21904/weken/2022/v7/i2/173014

The danger of re-identification can be minimized by using data anonymization methods including de-identification and pseudonymization, which include the removal or obfuscation of personally identifying information.

To protect patient confidentiality and meet legal standards, consent management is essential. The framework has to provide features for collecting and administering patient permission to share data. Patients can choose the nature, length, and intended use of data sharing by using smart contracts to express their choices. Patients should be able to easily see who has access to their data using consent management systems and change or remove their permissions at any time. The confidentiality of individual patients is protected by adhering strictly to regulatory rules and consent regulations.

Auditability and Traceability: These two elements are essential to any reliable security system. The blockchain technology incorporated into the architecture keeps a permanent and auditable ledger of all data exchanges and transactional activity. In the event of a security breach, forensic analysis may be performed with ease because to the blockchain's capacity to track every transaction back to its original source. Data access and sharing operations may be efficiently audited because to the blockchain's openness and immutability.

Even with stringent precautions, there is always a chance that a security event or data breach may occur. Protocols for handling incidents and data breaches should be clearly laid out within the framework. Data breaches can be contained and its effects mitigated by measures such as proactive monitoring, discovery, and reaction. In order to lessen the impact of an occurrence and keep people's faith in the system intact, prompt action and clear communication with those impacted are essential.

Healthcare requirements, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States or the General Data Protection Regulation (GDPR) in Europe, must be met for the framework to be considered compliant. Health information privacy and security are addressed in detail in these rules. The framework should be properly designed, implemented, and audited on a regular basis to assure compliance. In addition to reducing legal and reputational concerns, complying with rules preserves patients' privacy.

VI. SCALABILITY AND PERFORMANCE

The blockchain-enabled safe and scalable IoT data exchange architecture for healthcare places a premium on scalability and performance. The framework has to be able to efficiently handle and analyze huge volumes of healthcare data as the number of data generated by IoT devices continues to expand dramatically. Let's have a look at the most important factors and methods for the framework's scalability and performance:

The scalability of a system may be enhanced by using data splitting and sharding techniques. A distributed framework may shard data, or break it up into smaller pieces, and then spread them out throughout a network. This allows for parallel processing and reduces the load on individual nodes by having each shard process and store a subset of the data. Sharding and data partitioning make horizontal scalability possible, meaning that more network nodes may be added to handle more data without degrading performance.

Interoperability and Off-chain Data Storage The framework may use off-chain data storage options for data that is not mission-critical or doesn't need to be transparent in order to increase scalability. Cloud databases and distributed file systems, both of which are suitable for off-chain storage because of their scalability and speed, are two examples. The framework achieves this equilibrium between scalability and data integrity using a hybrid storage strategy that makes use of both on-chain and off-chain mechanisms.

Compressing data and using caching algorithms can increase efficiency by moving frequently accessed information to locations closer to the people who really use it.

DOI : 10.21904/weken/2022/v7/i2/173014

Latency and response times can be improved by caching data at several levels of the architecture, such as at the edge or within the data collectors. Compressing data before to transmission and storage can further reduce data volume for better system performance and lower bandwidth use.

Choosing the Right Consensus Mechanism The scalability and performance of a system can be greatly affected by the consensus mechanism used. Proof of Work (PoW) and other older consensus algorithms may struggle to keep up with growing transaction volumes because to their high computing requirements. Faster transaction validation and more scalability are available with alternative consensus algorithms like Proof of Stake (PoS) and Practical Byzantine Fault Tolerance (PBFT). The framework should choose a consensus method that guarantees the required security and trust features while also meeting the unique scalability and performance requirements.

Smart contracts play an important part in the framework, and their design can have an effect on scalability and performance, thus it's important that they be as well thought out as possible. When writing code for a smart contract, it's important to keep execution time and resource requirements as low as possible. Smart contracts may be optimized for execution speed by removing unnecessary code and minimizing the number of times an action is performed. Code may be reused more easily, redundancies are cut down, and scalability is increased when smart contracts are designed to be modular and reusable.

Optimization of the framework's network and infrastructure components can increase its scalability and performance. It is important to assess network bandwidth, latency, and throughput to make sure they can cope with the expected increase in data traffic. In order to avoid bottlenecks and get the most out of available resources, the framework may make use of load balancing strategies to spread the work over numerous nodes. Choosing the right hardware and cloud infrastructure may also aid performance enhancements by furnishing the required processing power and data storage space, respectively.

Maintaining scalability requires constant attention to performance metrics and fine-tuning of underlying code. Key performance parameters like response time, throughput, and resource usage should be measured with the use of monitoring tools and analytics that are built into the framework. Monitoring helps to identify performance bottlenecks and inefficiencies, which may then be optimized by using methods like code rewriting, database tuning, or infrastructure scalability. The framework's capacity to scale to accommodate the rising needs of healthcare data exchange depends on regular performance testing and benchmarking.

Future scalability is an important factor that must be taken into account while designing the framework. It has to be adaptable enough to handle the rapidly expanding quantities of both healthcare data and Internet of Things gadgets. Future growth and improvements may be made easier using modular and scalable designs, microservices, and containerization. In addition, as they develop, promising new tools like sharding protocols, state channels, and sidechains might be investigated to see whether they can further improve scalability.

VII. USE CASES AND APPLICATIONS

Numerous use cases and applications exist for the revolutionary blockchain-enabled safe and scalable IoT data exchange platform for healthcare. The framework provides safe, efficient, and transparent methods of sharing information by harnessing the potential of blockchain technology and Internet of Things devices. Here are some of the most important scenarios and uses:

Sharing Electronic Health Records (EHR): The framework can allow for the safe and efficient transfer of EHRs across medical facilities. When patients provide their permission, healthcare providers can safely disclose their patients' medical records, including information about their past conditions, current treatments, and any drugs they may be taking. As a result, healthcare providers will be able to make more well-informed decisions and deliver improved continuity of care because to increased interoperability and collaboration.

DOI : 10.21904/weken/2022/v7/i2/173014

Blockchain-enabled data exchange has the potential to greatly improve the efficiency of clinical trials and research. Accessing and analyzing patient data from many sources in a safe environment helps researchers find good study participants. Consent management may be automated with the use of smart contracts, protecting patients' confidentiality at every stage of the study process. In addition, the blockchain's immutability guarantees the accuracy and verifiability of research data, fostering openness and confidence in clinical studies.

The framework can provide remote patient monitoring, which is the collection of real-time health data from patients' homes via Internet of Things devices. Continuous monitoring and safe transmission of vital indicators, including heart rate, blood pressure, glucose levels, and activity levels, to healthcare specialists is now possible. Care can be managed proactively, health problems can be identified sooner, and treatment can begin sooner. The framework's emphasis on decentralization and security means that patient information may be kept private and safe.

Blockchain technology has the potential to increase transparency and traceability in the pharmaceutical supply chain. Using the blockchain, a permanent and verifiable record of the production and distribution processes may be kept. This helps to reduce the prevalence of fake drugs on the market and boosts overall medication safety. Internet of Things devices can track and monitor temperature-sensitive drugs in transit to guarantee their safety and effectiveness.

When it comes to health insurance claims and fraud detection, the framework can help by allowing for the safe and efficient transfer of pertinent patient data between insurance companies, medical institutions, and individual policyholders. Smart contracts have the potential to streamline the claims process by automating the verification and settlement of claims. The immutability of the blockchain ensures that claim transactions cannot be altered, which is a significant step toward reducing the prevalence of fraud. As a result, claims are processed more accurately and fraud is reduced (Chen, 2021).

Effective public health surveillance and disease outbreak control can benefit from the sharing of data made possible by the blockchain. Data from Internet of Things (IoT) devices, such as wearables or environmental sensors, may be gathered and analyzed in real time without compromising privacy or security. Because of this, illness outbreaks may be identified quickly, and appropriate measures can be taken to prevent further spread. Improved disease surveillance and prevention can result from the framework's transparent and decentralized design, which encourages data exchange across public health organizations, academics, and healthcare providers.

Through the safe transfer of genetic data, treatment records, and patient preferences, the framework can facilitate customized medicine and aid in the development of individualized treatment plans. Using this information, doctors may give patients care that is specifically designed for them. Patient autonomy over their genetic data may be protected through the use of smart contracts, which can automate the permission and data sharing process. This paves the way for precision medicine methods, which in turn allow for more tailored medical care.

The framework has the potential to pave the way for health data markets, where individuals may make informed decisions about whether or not to share their health information with third parties including insurance companies, pharmaceutical firms, and researchers. Patients can be rewarded or encouraged with tokens or other blockchain-based incentives for sharing their data securely. This allows for protected research and innovation based on patient data without compromising confidentiality or permissions

VIII. IMPLEMENTATION CONSIDERATIONS

Hardware and Software: To store, process, and transmit healthcare data, the framework requires a scalable and reliable hardware and software infrastructure. Data created by IoT devices is expected to grow exponentially, thus it is essential that adequate processing resources, storage space, and network bandwidth be made available.

DOI : 10.21904/weken/2022/v7/i2/173014

The framework's needs for scalability, dependability, and security should inform the choice of hardware, cloud infrastructure, or edge computing solutions.

Interoperability and standards are essential to the effective rollout of the framework. To facilitate easy integration and data interchange, the healthcare industry, IoT device makers, and data consumers should all use the same protocols and file formats. Interoperability across healthcare systems, IoT devices, and data formats is possible because to the development of standards like Health Level 7 (HL7), FHIR (Fast Healthcare Interoperability Resources), and DICOM (Digital Imaging and Communications in Medicine).

Electronic health record (EHR) systems, laboratory information systems, and clinical decision support systems are just a few examples of how the framework could be built to function in tandem with preexisting healthcare IT infrastructure. In order to allow data interoperability and simplify the interchange of information between the blockchain framework and current systems, APIs (Application Programming Interfaces) and middleware can be used. Careful integration is required to guarantee accurate data and maintain the continuity of existing processes.

Integral to the success of the framework's execution is careful attention to data governance and regulatory compliance. The administration of data access, sharing, and permission has to be governed by clear policies and processes. Protecting patient privacy and being on the right side of the law necessitates adhering to healthcare rules like HIPAA and the General Data Protection Regulation. Protecting private medical information requires the use of tools like encryption, access restrictions, and audit trails.

Implementation and acceptance of the framework depend critically on the quality of the user experience and the quality of training provided to users. Designing user interfaces and processes so that healthcare providers, patients, and other stakeholders can quickly learn and utilize them is essential. The functionality, data exchange methods, and security best practices of the framework should be made clear to users through in-depth training programs and instructional materials. Actively seeking and incorporating user feedback into the system's iterative improvement is essential.

To make sure it can manage the expected data and user loads, the framework has to be put through extensive scalability and performance testing before it is released. Benchmarking, performance load testing, and stress testing can help you find performance bottlenecks and fix them. The framework's scalability and performance should be verified using realistic test scenarios, such as the creation of simulated data from IoT devices.

Participation from a wide range of participants in the healthcare ecosystem is essential for a smooth rollout of the framework. Participants in the design, development, and implementation phases should include healthcare practitioners, IoT device makers, data consumers, regulatory authorities, and patients. To address issues, collect requirements, and maintain alignment with the needs of all stakeholders, regular communication, workshops, and feedback sessions should be held. Collaboration increases buy-in, trust, and accountability for the framework's success.

The security posture of the framework may be evaluated and vulnerabilities or flaws can be found through periodic security audits and continuous monitoring. The identification and correction of security flaws can be aided through penetration testing, code reviews, and vulnerability assessments. The framework's architecture, network, and applications must be continuously monitored in order to detect and respond to possible security events in a timely manner. Newly found vulnerabilities can be lessened by promptly applying security updates and fixes.

Iterative Development and Pilot ProjectsThe framework's functionality, usability, and scalability may be validated in real-world healthcare settings through the use of pilot projects. The framework should be continually refined and improved based on feedback from pilot initiatives. The framework may be made suitable for the specific needs of various healthcare organizations and use cases by learning from the experiences gained through trial implementations.

DOI : 10.21904/weken/2022/v7/i2/173014

Long-Term Sustainability and Governance: The framework's long-term sustainability and governance should be carefully considered. The framework's development, support, and growth should be guaranteed by establishing long-term financing models, maintenance plans, and governance structures. Long-term success and widespread adoption of the framework within the healthcare sector depend, in part, on cooperation with industry consortia, standards organizations, and regulatory agencies.

IX. EVALUATION AND CHALLENGES

The efficacy, opportunities for improvement, and alignment with the targeted outcomes of the blockchain-enabled safe and scalable IoT data sharing framework for healthcare must be evaluated. The review process entails tracking a number of KPIs (key performance indicators), hearing from key players, and solving any problems that may crop up. Let's look at the framework's assessment features and possible roadblocks:

The performance evaluation considers the effectiveness, scalability, and responsiveness of the framework. Data processing speed, transaction throughput, network latency, and system availability are just some of the key performance indicators (KPIs) that may be monitored and compared to industry standards. The framework's responsiveness to varying loads may be tested using load and stress simulations. Any performance bottlenecks should be identified and eliminated through continuous monitoring and improvement.

The success of the framework depends heavily on the level of user happiness and the rate of adoption. User happiness, usability, and experience may be gleaned via surveys, interviews, and other feedback channels. Suggestions for enhancement, usability problems, and training requirements may all be uncovered with input from healthcare providers, patients, and other interested parties. Metrics like adoption rates, user engagement, and user approval may be tracked to evaluate the extent of adoption and locate avenues for increasing that rate.

The security controls in the framework, any vulnerabilities, and the degree to which security best practices and regulatory requirements are being followed should all be subject to regular audits and evaluations. Potential security flaws can be found by penetration testing, vulnerability scanning, and code reviews. Audits of data privacy can check for infractions of privacy laws and assess how well safeguards are working. In order to keep the shared healthcare data secure, private, and reliable within the framework, it is crucial that the highlighted security and privacy vulnerabilities be resolved.

The success of the framework in enhancing patient care, treatment results, and operational efficiency may be gauged by assessing its influence on healthcare outcomes. Metrics such as treatment error rates, diagnostic precision, patient access, and healthcare expenditures may all be tracked and compared to industry standards. The effect of the framework on patient outcomes and healthcare quality may be better understood through case studies, real-world deployments, and data analysis.

Evaluating stakeholder participation and collaboration is essential for making sure the framework meets the requirements of all relevant parties. Stakeholder satisfaction, potential areas of collaboration, and obstacles may all be evaluated through regular feedback sessions, workshops, and collaborative forums. The framework's success in encouraging data sharing and innovation through cooperation may be gauged by the amount of involvement and engagement of healthcare organizations, IoT device makers, data consumers, and regulatory agencies.

Problems with the Framework's Application:

Several obstacles may arise during implementation of a blockchain-enabled safe and scalable IoT data exchange framework for healthcare, such as:

When dealing with massive amounts of healthcare data and an ever-increasing number of IoT devices, it might be difficult to achieve scalability and optimal performance.

DOI : 10.21904/weken/2022/v7/i2/173014

Maintaining performance as the framework grows in size requires careful attention to data processing, network optimization, and resource allocation. These issues can be mitigated by the use of modern architectural design patterns and technologies that allow for horizontal scalability and effective data partitioning (Sharma, 2017).

Due to the wide variety of healthcare systems, equipment, and data formats, interoperability continues to be a significant concern. Adopting established protocols, data formats, and interoperability frameworks is essential for ensuring the smooth integration and flow of data between various healthcare systems, IoT devices, and data consumers. This obstacle may be solved with the aid of industry-wide collaboration and strict adherence to healthcare standards.

Data privacy laws (including HIPAA and GDPR), patient consent, and data security are just a few of the rules and laws that the healthcare business must adhere to. It can be difficult and time-consuming to adopt the framework while also ensuring that all applicable laws and rules are followed. These compliance issues can be mitigated by the adoption of strong data governance rules, the use of suitable security measures, and the incorporation of privacy-by-design principles.

Management of Data Ownership and Consent: Data ownership and consent management inside the framework can be a challenging problem. Patients should be allowed to see their own health records and provide or remove permission for data sharing at any time. These problems may be overcome and data sharing authorized by patients only through the development and implementation of permission management methods like smart contracts and decentralized identifiers.

Gaining buy-in from key players and getting the word out about the framework may be difficult. For the framework to be widely adopted, it is essential to overcome opposition to change, resolve concerns about data security and privacy, and prove the framework's worth. Collaborative efforts, stakeholder involvement, and the presentation of compelling use cases may all contribute to the development of trust and the acceleration of adoption.

X. CONCLUSION

In conclusion, a viable solution to the problems caused by conventional data sharing techniques is the creation of a blockchain-enabled safe and scalable IoT data sharing framework for healthcare applications. This framework provides a safe and effective environment for exchanging and managing healthcare data generated by IoT devices by capitalizing on the distinctive characteristics of blockchain technology, such as decentralization, immutability, and transparency.

By offering strong security measures, maintaining data integrity and privacy, fostering interoperability, and able to accommodate the rising amount and diversity of IoT-generated healthcare data, the proposed framework overcomes the constraints of current data sharing techniques. Several crucial benefits for healthcare applications may be realized with the addition of blockchain technology to the framework.

Integrating blockchain technology has several advantages, but one of the most notable is the security of data. Data in a blockchain cannot be changed without the agreement of all participants due to the distributed nature of the technology. Because of this, the shared healthcare data may be trusted and used for important tasks including diagnosis, treatment, and research. To further ensure that sensitive healthcare data remains private and secure, the framework makes use of cryptographic algorithms and smart contracts.

In addition, smart contracts enable transparent and auditable data exchanges within the framework. Smart contracts are legally binding contracts that carry out their terms automatically. Smart contracts may create and implement data sharing policies, consent management, and access control methods in the context of healthcare data sharing. Automating these steps eliminates the need for go-betweens, speeds up information exchange, and lessens the likelihood of mistakes or ill intent on the part of human participants.

DOI : 10.21904/weken/2022/v7/i2/173014

The blockchain's distributed and decentralized architecture helps it scale well and run efficiently. When it comes to healthcare data, the proliferation of IoT devices can overwhelm traditional centralized data exchange platforms. In contrast, horizontal scalability is a feature of the blockchain, making it possible for the network to support a high number of nodes and disperse the processing of a huge volume of data. To facilitate real-time decision making and improve healthcare systems' overall efficiency, scalability is essential for data storage, retrieval, and analysis.

In addition, the architecture encourages communication between various medical networks, Internet of Things gadgets, and data users. Because healthcare institutions and platforms use diverse data formats, protocols, and systems, interoperability has been an ongoing problem. The framework enables trouble-free integration and data sharing between separate systems by employing common blockchain protocols and data exchange formats. This compatibility promotes teamwork, makes in-depth data analysis possible, and opens the door to novel healthcare applications and studies.

However, there are obstacles to putting the suggested framework into practice. There are a number of obstacles that must be overcome, including interoperability with current healthcare systems, regulatory compliance, data ownership and consent management, and stakeholder trust building. In addition, scalability and performance optimization are critical to manage the constantly expanding quantity of healthcare data and the expanding assortment of IoT devices.

REFERENCES

[1] G. Atlam, Alenezi, H. a., Alassafi, A. a., Wills, M. a., & Gary. (2018, 06). Blockchain with Internet of Things: Benefits, Challenges and Future Directions. International Journal of Intelligent Systems and Applications, 10.

[2] Chen, C.-L. a.-Y.-J.-T.-C.-M. (2021, 8). A Traceable Online Insurance Claims System Based on Blockchain and Smart Contract Technology. Sustainability, 13, 9386.

[3] Denning, Tamara, Borning, Alan, Friedman, Batya, . . . William. (2010, 04). Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices. Conference on Human Factors in Computing Systems - Proceedings, 2, 917-926.

[4] Goble, Carole, Stevens, & Robert. (2008, 03). State of the nation in data integration for bioinformatics. Journal of biomedical informatics, 41, 687-93.

[5] Kim, Soohyeong, Kwon, Yongseok, Cho, & Sunghyun. (2018, 10). A Survey of Scalability Solutions on Blockchain., (pp. 1204-1207).

[6] Li, Xiao, Wu, & Weili. (2022, 12). Recent Advances of Blockchain and Its Applications. Journal of Social Computing, 3, 363-394.

[7] Mohammed, & Ishaq Azhar. (2021). IDENTITY & ACCESS MANAGEMENT SYSTEM BASED ON BLOCKCHAIN. SSRN Electronic Journal, 8, 477-483.

[8] Novo, & Oscar. (2018, 3). Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. 5, 1184-1195.

[9] Rajput, Li, A. a., Ahvanooey, Q. a., & Milad. (2021, 02). A Blockchain-Based Secret-Data Sharing Framework for Personal Health Records in Emergency Condition. Healthcare, 9.

[10] Rayan, Rehab, Tsagkaris, Christos, Romash, & Iryna. (2021). The Internet of Things for Healthcare: Applications, Selected Cases and Challenges.

[11] Sharma, S. K. (2017, 03). Live Data Analytics With Collaborative Edge and Cloud Processing in Wireless IoT Networks. IEEE Access, 1-1.

[12] Wu, Yichang, Qiao, Yuansong, Ye, Yuhang, . . . Brian. (2019). Towards Improved Trust in Threat Intelligence Sharing using Blockchain and Trusted Computing., (pp. 474-481).

[13] Zheng, Zibin, Xie, Shaoan, Dai, Hong-Ning, . . . Huaimin. (2017, 6). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends

DOI : 10.21904/weken/2022/v7/i2/173014