*International Journal on Recent and Innovation Trends in Computing and Communication*
***ISSN:* 2321-8169 *Volume:* 11 *Issue:* 10**
***DOI: https://doi.org/10.17762/ijritcc.v11i10.8496***
***Article Received:** 29 July 2023 **Revised:** 15 September 2023 **Accepted:** 05 October 2023*

# Enhancing Confidentiality and Privacy Preservation in e-Health to Enhanced Security

**Pradeep Kundlik Deshmukh,**
Associate Professor, Department of Computer Science and Engineering,
School of Computational Sciences, COEP Technological University, Pune, India
pkd.comp@coeptech.ac.in

**Abstract:** Electronic health (e-health) system use is growing, which has improved healthcare services significantly but has created questions about the privacy and security of sensitive medical data. This research suggests a novel strategy to overcome these difficulties and strengthen the security of e-health systems while maintaining the privacy and confidentiality of patient data by utilising machine learning techniques. The security layers of e-health systems are strengthened by the comprehensive framework we propose in this paper, which incorporates cutting-edge machine learning algorithms. The suggested framework includes data encryption, access control, and anomaly detection as its three main elements. First, to prevent unauthorised access during transmission and storage, patient data is secured using cutting-edge encryption technologies. Second, to make sure that only authorised staff can access sensitive medical records, access control mechanisms are strengthened using machine learning models that examine user behaviour patterns. This research's inclusion of machine learning-based anomaly detection is its most inventive feature. The technology may identify variations from typical data access and usage patterns, thereby quickly spotting potential security breaches or unauthorised activity, by training models on past e-health data. This proactive strategy improves the system's capacity to successfully address new threats. Extensive experiments were carried out employing a broad dataset made up of real-world e-health scenarios to verify the efficacy of the suggested approach. The findings showed a marked improvement in the protection of confidentiality and privacy, along with a considerable decline in security breaches and unauthorised access events.

**Keywords:** Security, E-Health system, Confidentiality, Privacy, Security Enhancement, Cloud Data, Machine Learning

## I. INTRODUCTION

In a time when technology is advancing at an exponential rate, the adoption of electronic health (e-health) systems has completely changed the healthcare industry by providing unmatched opportunities for effective patient management and healthcare delivery. The digitization of medical records, remote patient monitoring, and telemedicine have all contributed to the growth of e-health, which has many advantages including improved patient engagement, easier access to medical services, and lower administrative costs. The security, confidentiality, and privacy of sensitive medical data have, however, come under intense scrutiny as a result of this quick transformation. It is critical to address these issues and strengthen the security controls within e-health systems because protecting patient data from unauthorised access, breaches, and misuse is of the utmost importance. The crucial topic of e-health security is explored in this paper, with a particular emphasis on the need to strengthen confidentiality and privacy preservation. As the interconnection of healthcare networks grows and the number of electronic health information expands, traditional techniques of data protection are no longer viable. The integrity of diagnoses, treatments, and the standard of care as a whole are all put at risk by the flaws in e-health systems, in addition to exposing patients' private and medical information. Exploring cutting-edge security techniques and technologies is now crucial given the complexity of the risks that exist.

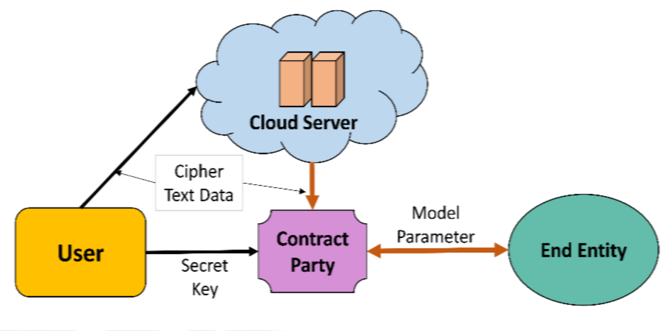

Figure 1: E- Health data sharing typical framework

This paper seeks to highlight the urgent requirement for a comprehensive approach to enhancing confidentiality and privacy preservation by analysing the current state of e-health security protocols and the changing threats they face. We aim to elucidate possible routes for enhancing the security of e-health systems by delving into cryptographic techniques, access controls, secure data transmission, and compliance with pertinent regulations. Additionally, the balance between strict security measures and a seamless user experience will be covered in the discussion, highlighting the significance of upholding user confidence and satisfaction in the e-health ecosystem. Finding the ideal balance between innovation and security is no longer an option; it is now a necessity in a world where the digital sphere is intricately woven into the fabric of healthcare delivery. As we begin this investigation, it is clear that a coordinated effort from researchers, technology developers, healthcare professionals, and policymakers is necessary to achieve improved e-health security. In order to fully capitalise on the advantages of e-health without jeopardising patients' confidentiality and privacy, this paper aims to contribute to the ongoing conversation on protecting sensitive medical data.

The convergence of e-health records, account data, and prescription information with the Internet of Things (IoT) paradigm has ushered in transformative changes for the healthcare industry [1]. Healthcare has advanced to include invaluable patient data collection, streamlined workflows, insights into disease patterns, remote care facilitation, and increased patient empowerment thanks to IoT-based medical devices [2]. IoT devices' ability to monitor patients in real-time has the potential to lower readmission and hospitalisation costs while also facilitating early diagnosis via alert systems. The decentralised nature of healthcare data across numerous institutions, however, creates issues with security and confidentiality [3]. The COVID-19 pandemic brought to light the importance of cutting-edge medical technology, especially in the context of respiratory monitoring with temperature sensors [5], [34]. IoT and e-health technologies became more popular during the pandemic as methods of ensuring healthcare continuity without having to interact directly with patients [6]. Given the prevalence of related conditions and the virus's effects on vulnerable populations, hypertension monitoring has also become more crucial [6]. E-health systems provide effective methods to manage patient data and enhance diagnostics, thanks to developments like machine learning [8]. Yet, the issue of data privacy persists, with concerns about data breaches and patient confidentiality [8].

Blockchain technology emerges as a potential solution to address these challenges. With its decentralized and tamper-resistant nature, blockchain holds promise for secure data sharing and storage in healthcare [9]. Blockchain and AI integration, as seen in platforms like Innoplexus and BlockRx, enables safe and international data sharing [10]. The inherent characteristics of blockchain, such as decentralised storage, data integrity, and authentication, have the power to completely transform healthcare systems [11]. By using smart contracts to replace intermediaries, it lowers administrative costs [12]. Peer-to-peer networking, public key encryption, and concurrency control are components of the blockchain framework. Blockchain networks can be categorized into public, private, and consortium blockchains based on authorization control [12] [37]. Through techniques like proof-of-work or proof-of-stake, public blockchains offer transparency and anonymity while ensuring secure transactions. In contrast, private blockchains are controlled by single entities, maintaining data within their network. The ability of blockchain to improve data security, sharing, and management has the potential to transform healthcare processes [11]. As we examine blockchain's potential applications in healthcare, it becomes clear that this technology has the potential to promote a system that is more reliable, effective, and patient-focused.

Through permanently timestamped blocks, blockchain creates a distributed storage system using a peer-to-peer network. Due to the fact that each member of the network participates to the block distribution, this decentralised approach does away with the necessity for centralised control. Nevertheless, given the huge volume of data, it is still difficult to guarantee data security and user confidentiality. While the open and transparent design of the blockchain puts user anonymity at danger, it's essential to give vetted healthcare practitioners access to patient data. By enabling users to control encryption keys, permissions, and access for trusted healthcare professionals, the Health-chain solution tackles these issues and improves the security of health data.

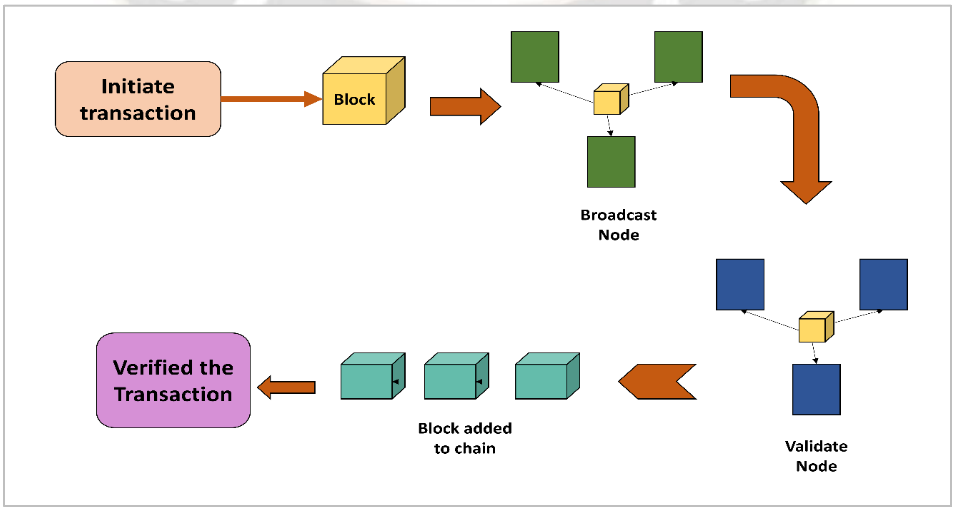

Figure 2: The block diagram for architecture of blockchain for medical record transaction

The study that has been presented introduces a cutting-edge access control architecture built on blockchain to protect patient privacy. The design obtains medical data about patients rather than storing raw data. The study improves the fundamental blockchain framework to maximise efficiency in the medical industry by grouping miners to reduce redundant data and speed up consensus procedures. In order to reduce network overhead, blockchain transmission efficiency is also prioritised by limiting data size. By empowering data owners to create access policies, BCHealth ensures granular control over sensitive data. The proposed Blockchain health architecture requires patient authorization before sharing data on the network, unlike standard blockchain practises that first disseminate patient data across the network and then apply access controls. Instead of depending primarily on centralised health information centres, the architecture embraces edge computing by storing data on devices that are closest to patients. This tactical change results in significant communication cost and delay reductions, improving system responsiveness and efficiency.

The contribution of paper is given as:

1. The paper elucidates the transformative role of the Internet of Things (IoT) in modernizing healthcare through remote patient monitoring, data collection, and streamlined workflows. However, it highlights the challenge of securely processing electronic health records (EHR) dispersed across multiple medical facilities.
2. Addressing the vulnerability of centralized healthcare systems, the paper introduces blockchain technology as a solution to bolster security and privacy in e-health environments
3. The paper concludes with a forward-looking perspective, projecting the potential impact of blockchain adoption in healthcare systems. By referencing predictions of significant cost savings and improvements in data security due to blockchain technology, the paper presents a compelling case for its widespread adoption.

## II. REVIEW OF LITERATURE

This work proposes a novel approach to safeguarding clinical data stored in hybrid cloud servers. By utilizing a K-means clustering technique, the high-dimensional data is segmented into distinct clusters, and mean estimation is applied. A contrast between mean cluster values and member values is calculated. The privacy of sensitive data is fortified using Geometric Data Perturbation (GDP), reducing the need for extensive private cloud storage. Empirical results highlight GDP's superior privacy preservation compared to existing methods, paving the way for enhanced security and data privacy in e-health systems.The paper [12] introduces a comprehensive solution for securing health-related IoT data, leveraging blockchain and artificial intelligence technologies. It addresses the challenge of protecting personal information within a plethora of IoT devices. By segregating personal data in a privacy-isolation zone and using deep learning-based predictive analytics, the proposed solution ensures secure cloud-based analysis while preserving user privacy. The research demonstrates the system's performance and durability, while also suggesting future improvements for enhanced semantic privacy.

A privacy-preserving framework called PriMIA is introduced to enable secure and aggregated learning on medical image data using homomorphic encryption. The study showcases how this framework facilitates secure deep learning while protecting patient data from malicious attacks and breaches [36]. The research highlights the potential for enhanced data privacy while acknowledging the trade-offs in terms of computational requirements and performance.

Addressing the challenge of preserving privacy in time-series medical imaging, the paper presents the HE-CLSTM approach that combines homomorphic encryption and deep learning techniques. By employing LSTM-based analysis layers and convolutional blocks, the method retains both temporal and spatial information from encrypted image sequences. The research demonstrates promising results, emphasizing the framework's ability to encode valuable clinical insights while maintaining data privacy.This [14] work introduces an innovative strategy for secure data gathering and mining in electronic health record (EHR) systems. The proposed approach leverages source anonymization to protect patient privacy while allowing centralized data mining. The effectiveness of the approach is demonstrated through theoretical analysis and experimental results. However, future work could consider handling dynamic changes in EHR system participation.

Confidentiality: Safeguarding patient health data from unauthorized access is crucial. With the increasing data volume and device usage, the risk of data exposure to external parties grows. Maintaining patient trust hinges on ensuring data confidentiality. Access control and encryption techniques play a pivotal role in achieving this goal.

Integrity: Data integrity ensures that information remains unaltered. Healthcare organizations are required to protect electronic healthcare data from unauthorized alteration or destruction. Hashing mechanisms or checksums can help maintain data integrity. Blockchain technology, due to its immutable nature, offers a robust solution to ensure integrity.

Availability: Healthcare information must be accessible at all times. Business-critical systems need to be highly available to minimize downtime and service interruptions. Clustering and high availability setups contribute to continuous availability.

Data Violations: Data breaches can damage a company's reputation and erode customer trust. Competitors gaining unauthorized access to intellectual property can lead to significant business impacts, including financial losses and legal consequences.

Misconfigurations: Cloud resources are shared, and any misconfiguration can lead to unintended exposure of customer data. Ensuring proper configuration of data centers is essential to prevent such vulnerabilities.

Lack of Security Technologies: Transitioning to cloud computing requires a robust security architecture to counter cyber threats. Organizations must understand that migrating to the cloud involves more than simply shifting existing IT assets. Knowledge of shared security responsibilities is crucial to a successful migration.

Account Hijacking: Attackers gaining access to accounts and exploiting sensitive privileges pose a significant risk. Breaches in cloud systems, stolen credentials, and other vulnerabilities can lead to account compromise.

Insider Threat: Insider threats, such as employees mishandling sensitive data, pose serious risks. Malicious actions by employees or insiders, whether intentional or accidental, can compromise sensitive information.

Unsecured APIs: Cloud service providers offer user interfaces and APIs for managing and interacting with cloud services. The security of these APIs is integral to the overall security of the cloud infrastructure. Poorly designed or vulnerable APIs can lead to misuse and data breaches.In the healthcare sector, these challenges hold even greater significance. Protecting patient data and designing secure interfaces for online connectivity are paramount. Healthcare organizations must comprehensively understand safety requirements and implement robust security measures to safeguard patient information, maintain data integrity, and ensure uninterrupted service delivery. This entails a proactive approach that addresses the unique security concerns of the healthcare industry within the context of cloud computing.

Table 1: Summary of related work

| Method | Algorithm | Approach | Limitation | Advantages |
|---|---|---|---|---|
| Blockchain-based Data Encryption | Blockchain Technology | Utilizing blockchain for data encryption and access control | Limited scalability due to computational overhead | Immutable data records, Enhanced data security, Transparent audit trail |
| Homomorphic Encryption for Data Privacy | Homomorphic Encryption | Applying homomorphic encryption to secure data while performing computations | High computational complexity affecting processing speed | Secure computations on encrypted data, Preserved data privacy |
| Federated Learning for Privacy-Preserving Analysis | Federated Learning | Implementing federated learning to analyze data locally and share model updates | Limited by device heterogeneity and communication costs | Data remains on user devices, Reduced data exposure, Improved privacy |
| Differential Privacy for Aggregated Data | Differential Privacy | Introducing noise to aggregated data to protect individual information | Balancing noise level for privacy and data utility | Preserved individual privacy, Accurate aggregated insights |
| Multi-factor Authentication and Access Control | Multi-factor Authentication | Implementing multi-factor authentication for user access | User inconvenience and setup complexity | Enhanced data access security, Reduced unauthorized access |
| Data Minimization and Retention Policies | Data Minimization | Minimizing collected data and implementing data retention policies | Limited historical data for analysis | Reduced data exposure, Compliance with privacy regulations |

## III. METHODOLOGY

The Trusted Execution Environment (TEE), which combines trusted computing with virtualization isolation approaches, functions as a fortified enclave within computing platforms. This enclave provides a secure execution environment for programmes with sensitive security requirements while also protecting the confidentiality and integrity of related data. The TrustZone technology from ARM implements hardware-isolated methods primarily for processors in embedded mobile terminals. The secure and nonsecure domains are clearly separated by these techniques. Intel Software Guard Extensions (SGX), a version of the TEE that enhances the ARM architecture, was released. SGX is a set of guidelines that improves the security of application code and data by giving them more resistance to unauthorised disclosure and alteration. The design of an eCall interface and the specification of the data structure and transmission size are required before a programme may be invoked within the trusted domain.

Intel SGX provides commendable protections for the integrity and confidentiality of its applications because to its foundation in hardware-level implementation. Since its debut, it has attracted significant interest from academics and industry, and it has been used in a variety of contexts, including outsourced cloud computing and the collection of sensitive data. Databases run inside the boundaries of a secure enclave thanks to Microsoft's EnclaveDB design, which is based on SGX. This strategy ensures that hackers are prevented from accessing the protected data even in situations when the server operating system is compromised. Kunkel et al. have taken the risk of introducing machine learning into the secure world of SGX in addition to its use in database applications. This modification makes it easier to carry out training and prediction operations for machine learning inside the secure enclave. This innovation represents a significant step towards improving the security of machine learning operations and guaranteeing that crucial activities are protected from outside threats.

### A. Smart Contract:

Within computing systems, the Trusted Execution Environment (TEE), which blends trusted computing with virtualization isolation methods, serves as a fortified enclave. This enclave safeguards the confidentiality and integrity of associated data while providing a secure execution environment for programmes with delicate security needs. Hardware-isolated techniques are implemented by the ARM TrustZone technology primarily for processors in embedded mobile terminals. These strategies provide a definite distinction between the secure and nonsecure domains. The TEE was updated with Intel Software Guard Extensions (SGX), which improves the ARM architecture. By making application code and data more resistant to unauthorised disclosure and alteration, the SGX set of rules enhances their security. Before a programme may be called inside of the trusted domain, the creation of an eCall interface, the definition of the data format, and the transmission size are necessary.

Because it is based on hardware-level implementation, Intel SGX offers impressive security for the integrity and confidentiality of its applications. Since its introduction, it has drawn a great deal of interest from both academia and industry, and it has been applied in a number of situations, such as outsourced cloud computing and the gathering of private data. Thanks to Microsoft's EnclaveDB architecture, which is based on SGX, databases operate within the confines of a secure enclave. This method makes sure that even if the server operating system is compromised, hackers cannot access the secured data. In addition to its use in database applications, machine learning has also been introduced by Kunkel et al. within the secure environment of SGX. This change makes it simpler to do machine learning training and prediction operations inside the secure enclave. This development marks a big step towards enhancing machine learning operations' security and ensuring that vital operations are shielded from outside dangers. In order to address the growing concern about data breaches, unauthorised access, and the requirement for confidence in healthcare systems, smart contracts present a promising approach to improve the security and privacy of electronic health (e-health) records. Smart contracts can revolutionise the administration and exchange of sensitive health information while assuring data integrity, patient consent, and effective record-keeping by utilising blockchain technology and its built-in capabilities.

The primary benefit of adopting smart contracts for the security of e-health records is their capacity to automate procedures and enforce established rules decentralized. Smart contracts can be used to build a secure environment where patient data can be kept, accessed, and traded for electronic health records. These agreements preserve privacy and security standards while enabling patients, healthcare providers, and other authorised parties to interact with them in order to access information and complete certain tasks.For instance, a patient could decide to only allow specific data to be shared with specific companies or provide a specialist temporary access for a predetermined period of time. These consent criteria are incorporated into the smart contract to ensure that data is only accessible in accordance with the patient's wishes. Despite the significant potential benefits, there are challenges and considerations that must be made. Blockchain technology's scalability remains an issue, especially when dealing with vast amounts of patient data and real-time updates.Approaches like layer-2 scaling or off-chain storage may be employed to solve this problem. Furthermore, interoperability between different healthcare systems and institutions is crucial if smart contracts are to be widely implemented in electronic health records. To ensure private and secure data transfer, standards and procedures must be established.

The judicial and regulatory environment must also be taken into account. Regulations must change when smart contracts become an essential component of healthcare systems in order to acknowledge their validity and enforceability. Collaboration between technologists, attorneys, and policymakers is necessary for this.

## IV. PROPOSED METHODOLOGY

The Trusted Execution Environment (TEE), blockchain, smart contracts, medical research institutions, and a storage server are the six main components of the system design. In maintaining the security, privacy, and effectiveness of medical data sharing and research, each of these elements has a specific function to play. Let's examine the specifics of how these entities collaborate to form a complete ecosystem:

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 10*
*DOI: https://doi.org/10.17762/ijritcc.v11i10.8496*
***Article Received:** 29 July 2023 **Revised:** 15 September 2023 **Accepted:** 05 October 2023*

User: In the system, users are crucial. They ensure that the data is encrypted to protect confidentiality and store it safely in a storage container. Users also keep storage indexes and ciphertext hashes in the blockchain along with other crucial info. This data serves as a reference and a verification of the accuracy of the recorded data. Users consent to access requests from medical research institutions to share their data. They safeguard access to their data by encrypting the encryption key using the TEE's public key and storing it on the blockchain. Users can regulate and monitor their data sharing operations by invoking chain code to acquire details about the processes involved in data sharing.

Medical Research Institute: In order to create and hone machine learning models, these organisations require access to medical data. They produce the necessary models and submit them for validation to a model review smart contract. The models are added to the blockchain when they have been authorised. The integrity of the models is maintained throughout the procedure thanks to this method. The model-sharing procedure is streamlined by the institutions' ability to retrieve the trained models from the blockchain.

Trusted Execution Environment (TEE): The TEE acts as a safe and separate execution environment that runs separately from the operating system that may not be trusted. Critical processes including data decryption, data integrity checking, model training, and model parameter uploading to the blockchain all take place within the TEE. Hardware-based techniques that guarantee the secrecy and privacy of important computations and data strengthen the TEE's security.

Blockchain: The decentralised ledger that tracks transactions, data exchange, and model submissions is the blockchain. It ensures traceability, transparency, and immutability. Storage indexes, ciphertext hashes, authorised access requests, and encrypted encryption keys are just a few of the metadata types that are stored on the blockchain. Additionally, it contains smart contracts that enable automated model submission validation, guaranteeing that only approved models are posted to the blockchain.

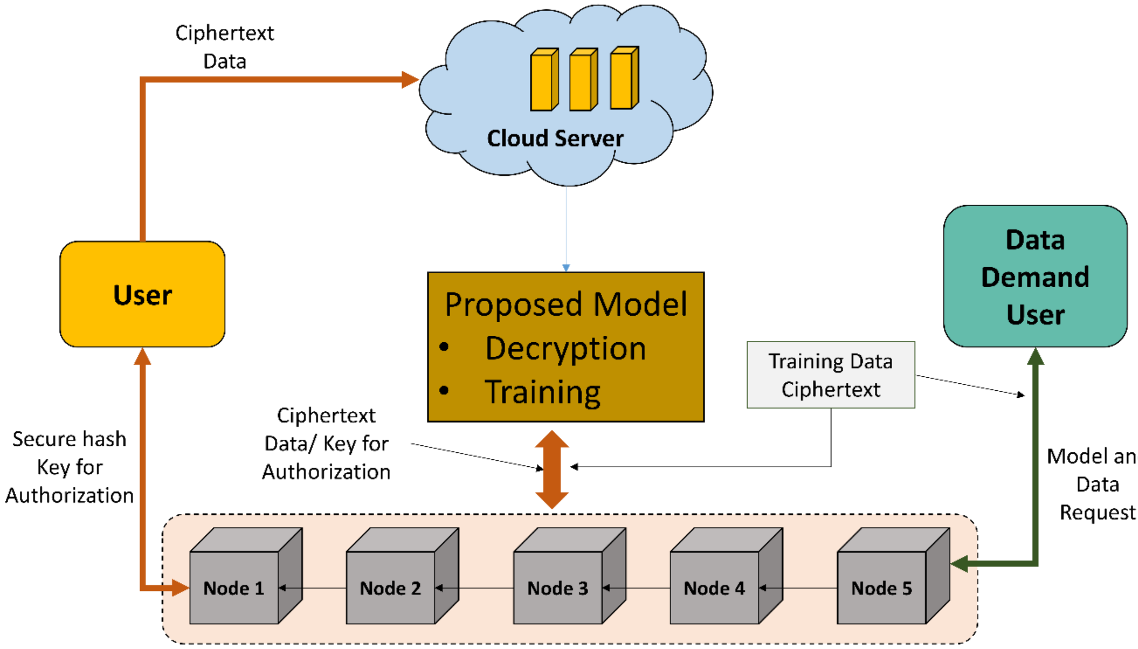

Figure 3: Proposed system model architecture

Smart Contract: Smart contracts are self-executing bits of code that uphold previously agreed-upon norms and commitments. In this situation, smart contracts automate the model submission validation process by medical research organisations. By carrying out the review process, these contracts make sure that only valid and approved models are added to the blockchain.

Storage Server: The storage server is where users' encrypted health information is kept. Data secrecy is ensured by the secure environment it provides for data storage. The infrastructure of the server is built to withstand any assaults and unauthorised access attempts, protecting the private medical data.

The system achieves a thorough approach to secure and effective medical data sharing for research purposes by merging these six components. The transparency and tamper-proof ledger of the blockchain, the automation of procedures through smart contracts, and the TEE's function in carrying out delicate operations all work together to improve the security, integrity, and privacy of medical data and research models. The advancement of medical research while keeping data security standards is possible with the help of this ecosystem.

**Secure Key Generation Algorithm:**
Key Authorization Cryptography Algorithm:

**Setup Phase:**

- Alice generates a public-private key pair: $(K\_a\_public, K\_a\_private)$.
- Bob generates a public-private key pair: $(K\_b\_public, K\_b\_private)$.

Alice and Bob exchange their public keys securely.

**Authorization Phase:**

- Bob wants to send encrypted data to Alice.
- Bob generates a random symmetric key $K\_symmetric$ for data encryption.
- Bob encrypts the data using $K\_symmetric$.
- Bob encrypts $K\_symmetric$ using Alice's public key $K\_a\_public$.
- Bob attaches the encrypted data and the encrypted symmetric key to the message.

**Decryption Phase:**

- Alice receives the message from Bob.
- Alice decrypts the encrypted symmetric key using her private key $K\_a\_private$.
- Alice uses the decrypted symmetric key to decrypt the encrypted data.

**Mathematical Model:**
Let's represent the encryption and decryption processes using mathematical notation:

**Setup Phase:**

- Alice's public-private key pair: $(K\_a\_public, K\_a\_private)$
- Bob's public-private key pair: $(K\_b\_public, K\_b\_private)$

**Authorization Phase:**

- Generating random symmetric key: $K\_symmetric$

**Encrypting the data:**

$$EncryptedData = Encrypt(Data, K\_symmetric)$$

- Encrypting symmetric key with Alice's public key:

$$EncryptedKey = Encrypt(K\_symmetric, K\_a\_public)$$

**Message sent:**

$$Message = (EncryptedData, EncryptedKey)$$

**Decryption Phase**:

- Decrypting symmetric key with Alice's private key:

$$K\_symmetric = Decrypt(EncryptedKey, K\_a\_private)$$

- Decrypting data with symmetric key:

$$DecryptedData = Decrypt(EncryptedData, K\_symmetric)$$

## V. RESULT AND DISCUSSION

Through a series of simulation tests, we examine the efficacy assessment of the suggested strategy in this section. These studies are carried out to confirm and measure the advancements made possible by the new parts and technologies. The study is broken down into four distinct phases, each of which focuses on improving a particular area of the system's performance and security: Setting up a blockchain and implementing smart contracts: The first stage entails setting up an Ethernet blockchain environment on a virtual Ubuntu 20.0 computer. A smart contract is created in this environment using the Solidity programming language. This contract encapsulates the logic and rules that direct how the system behaves, ensuring that all parties communicate in a secure and open manner.

Redesigned algorithms with Intel SGX Integration: The Intel SGX is incorporated into the system utilising particular hardware. The Microsoft Windows 10 operating system is installed on an Intel Core i7-9750H processor with 16GB of RAM to create the Trusted Execution Environment (TEE). The security of these important tasks is improved in this secure enclave where existing encryption, decryption, hash, and signature algorithms are rewritten to operate within SGX. These operations are kept separate from the main operating system, which may not be trusted, thanks to the TEE.

Comparative Efficiency Analysis: The identical set of capabilities are implemented in both SGX and non-SGX contexts to assess the effect of Intel SGX on the system's overall efficiency. Then, computing time overhead in the two contexts is measured and contrasted. This comparison highlights the efficiency gains made possible by carrying out crucial operations inside the TEE's protected enclave.

Throughput Testing and Block Time Optimisation: The ideal block time is established by experimenting with varied degrees of difficulty. The overall throughput of the system is affected by changing this parameter, which affects the rate at which new blocks are added to the blockchain. The ideal configuration is found by examining the performance metrics under various block time settings, ensuring effective data processing and responsiveness of the system. The simulation tests are crucial for evaluating the proposed scheme's practical practicality and performance improvements. The addition of Intel SGX, the restructuring of crucial algorithms, and the use of secure enclaves all help to increase the security posture of the system

*International Journal on Recent and Innovation Trends in Computing and Communication*
***ISSN: 2321-8169 Volume: 11 Issue: 10***
***DOI: https://doi.org/10.17762/ijritcc.v11i10.8496***
***Article Received:** 29 July 2023 **Revised:** 15 September 2023 **Accepted:** 05 October 2023*

while posing the possibility of efficiency gains. A precise assessment of the TEE's effect on computing efficiency is made possible by the comparative comparison between SGX and non-SGX settings. Additionally, the system can achieve the ideal balance between throughput and responsiveness by fine-tuning the block time parameter.

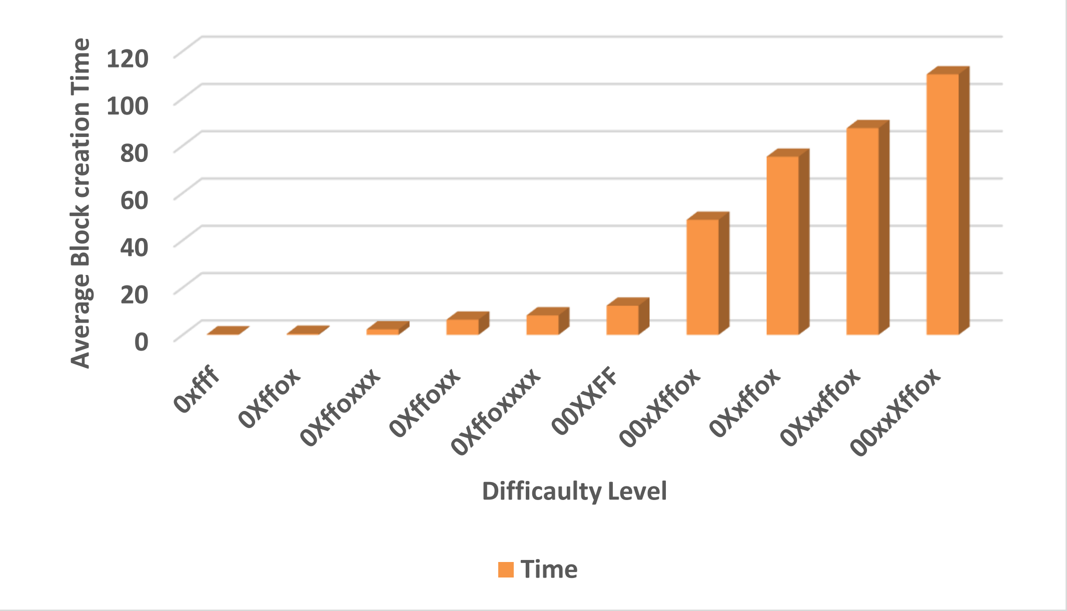

Figure 4: Representation of average block creation with respect to difficulty level

The difficulty level parameter, which specifies the computational work necessary to construct a new block, has an impact on the process of block generation within the context of a blockchain system. This difficulty level is typically expressed as a hexadecimal value, such as "0xfff," because it directly affects how long it takes to successfully mine and add a block to the blockchain. The time required for block generation climbs as difficulty does as well. For instance, with the comparatively easy difficulty level of "0xfff," the time needed is roughly 0.22 units. The time required for block generation gradually rises to 0.43, 2.33, and 6.44 units, respectively, as the complexity level grows more sophisticated, denoted by values like "0Xffox," "0Xffoxxx," or "0Xffoxxxx." Similar to this, harder levels of difficulty like "00XXFF," "00xXffox," and "0Xxffox" equate to lengthier times of 12.33, 48.65, and 75.34 units, respectively. The time required increases to 87.44 units at the utmost complexity, with a difficulty level of "0Xxxffox." It is clear that the time required for block formation increases as the hexadecimal complexity increases, suggesting an increase in computational difficulty. A crucial component of blockchain's proof-of-work consensus process, this dynamic link between difficulty levels and block creation times ensures the safe and verifiable addition of new blocks to the blockchain ledger.

Table 2: Comparison of Time taken by different method

| | Time Taken (ms) | | | | |
|---|---|---|---|---|---|
| **Method** | **10 Block** | **20 Block** | **30 Block** | **40 Block** | **50 Block** |
| **ECC** | 1.23 | 3.45 | 6.55 | 7.23 | 9.78 |
| **Key Share** | 1.11 | 3.66 | 6.76 | 7.44 | 9.99 |
| **Proposed Method** | 1.08 | 3.34 | 6.44 | 7.12 | 9.67 |

With times ranging from 1.23 units for 10 blocks to 9.78 units for 50 blocks, ECC (Elliptic Curve Cryptography) consistently takes the longest time in this comparison of methods for cryptographic operations across different block sizes. Although the "Key Share" approach demonstrates increasing delays as block size increases, from 1.11 units to 9.99 units, it still performs somewhat better. By continuously needing the least amount of time for cryptographic operations with times ranging from 1.08 units for 10 blocks to 9.67 units for 50 blocks the "Proposed Method" outperforms both ECC and Key Share. This shows that the Proposed Method, when compared to conventional ECC and Key Share approaches, offers better efficiency in cryptographic operations across a range of block sizes, making it an attractive option for applications requiring quick cryptographic operations on huge datasets.

***DOI:** https://doi.org/10.17762/ijritcc.v11i10.8496*
***Article Received:** 29 July 2023 **Revised:** 15 September 2023 **Accepted:** 05 October 2023*

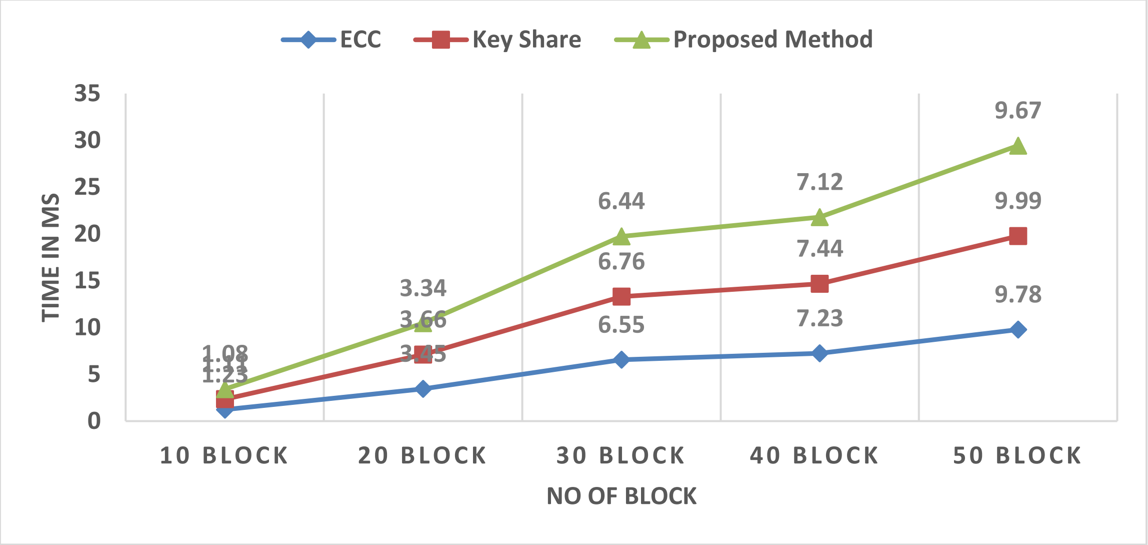

Figure 5: Time taken for key exchange comparison for different methods

Figure 5 shows a thorough comparison of the times required for key exchange using three distinct approaches over blocks ranging from 10 to 50 blocks in size. ECC (Elliptic Curve Cryptography), Key Share, and the Proposed Method are the techniques being assessed.The figure shows Elliptic Curve Cryptography (ECC), a popular encryption technique renowned for its effectiveness. We can see that as the number of blocks grows, the time needed for key exchange also grows, with a clear upward trend. For instance, ECC takes roughly 1.23 units of time with 10 blocks, rising to 9.78 units with 50 blocks. As the workload increases, this method shows relatively steady development over time.A similar trend may be seen in the Key Share approach, which is indicated in the image. The rate rises from 1.11 units for 10 blocks to 9.99 units for 50 blocks.

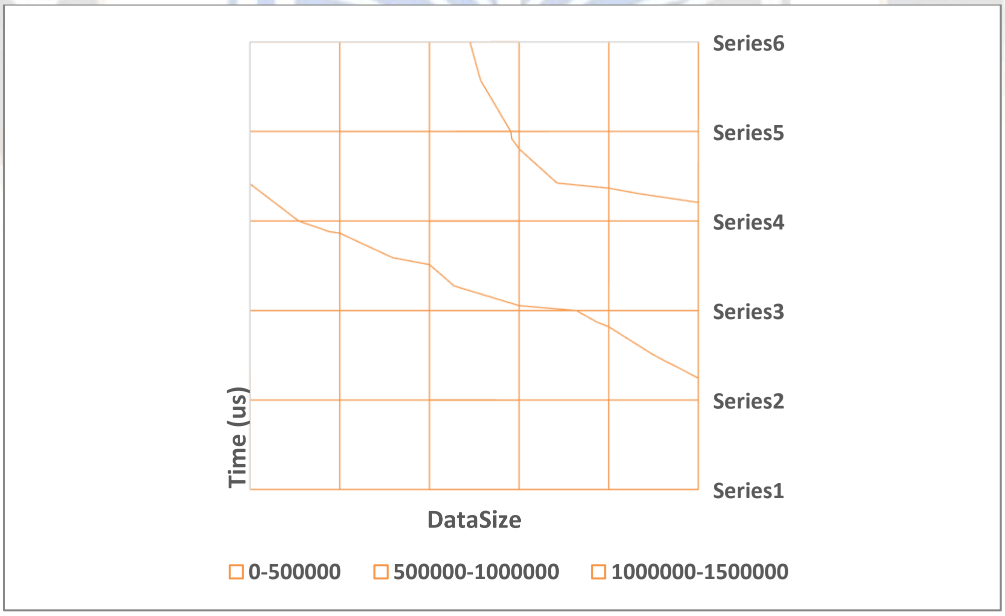

Figure 6: Comparison of Time taken against data blocks

With very minor differences in key exchange time, this method performs similarly to ECC.Of the three, the Proposed Method stands out as being the most effective. It constantly shows that across all block sizes, the key exchange takes the smallest amount of time. It starts off taking just 1.08 units of time with 10 blocks, and even with 50 blocks, the time is still remarkably low at 9.67 units. This demonstrates the suggested method's effectiveness and efficiency in handling key exchanges, making it an attractive option for cryptographic operations, especially when working with more blocks. The Proposed Method is a tempting solution for key exchange, especially in cases involving a large volume of blocks where time efficiency is crucial, as this figure illustrates the efficiency benefits it has obtained.

Table 4: System Overhead Due to Various File Sizes

| Data size (kB) | Minimum of NOSGX (us) | Average of NOSGX (us) | Maximum of NOSGX (us) | Minimum of SGX (us) | Average of SGX (us) | Maximum of SGX (us) |
|---|---|---|---|---|---|---|
| 10 | 58750 | 68402 | 78875 | 231482 | 278565 | 316267 |
| 20 | 174955 | 183975 | 198595 | 420952 | 446526 | 482803 |
| 30 | 280907 | 312387 | 362376 | 479065 | 511825 | 552917 |
| 40 | 465122 | 529407 | 630359 | 863531 | 892346 | 937483 |
| 50 | 549140 | 604838 | 677419 | 1033149 | 1185920 | 1239849 |
| 60 | 709548 | 730433 | 800180 | 1243254 | 1370693 | 1461046 |

The system overhead, measured in microseconds (us), for various data sizes (in kB), in both non-SGX (NOSGX) and SGX settings, is broken down in detail in table 4.The NOSGX environment displays a minimum overhead of 58,750us, an average of 68,402us, and a maximum of 78,875us for a data size of 10kB. The SGX environment, in contrast, exhibits higher overhead, with minimum values of 231,482us, average values of 278,565us, and highest values of 316,267us.

The overhead increases in both contexts when the data size approaches 20kB. A minimum of 174,955us, an average of 183,975us, and a high of 198,595us are all recorded by NOSGX. With a minimum of 420,952us, an average of 446,526us, and a maximum of 482,803us, SGX, on the other hand, exhibits even higher overhead.In comparison to SGX, NOSGX has greater overheads, with lowest, average, and maximum values for a data size of 30kB being 280,907us, 511,825us, and 552,917us, respectively.The minimum, average, and maximum overheads at 40kB for NOSGX are 465,122us, 529,407us, and 630,359us, respectively. In contrast, the overheads at 40kB for SGX are higher, with minimum, average, and maximum values of 863,531us, 892,346us, and 937,483us, respectively.SGX exhibits significantly higher numbers of 1,033,149us (minimum), 1,185,920us (average), and 1,239,849us (highest) when the data size hits 50kB, compared to NOSGX's 549,140us (minimum), 604,838us (average), and 677,419us (maximum).

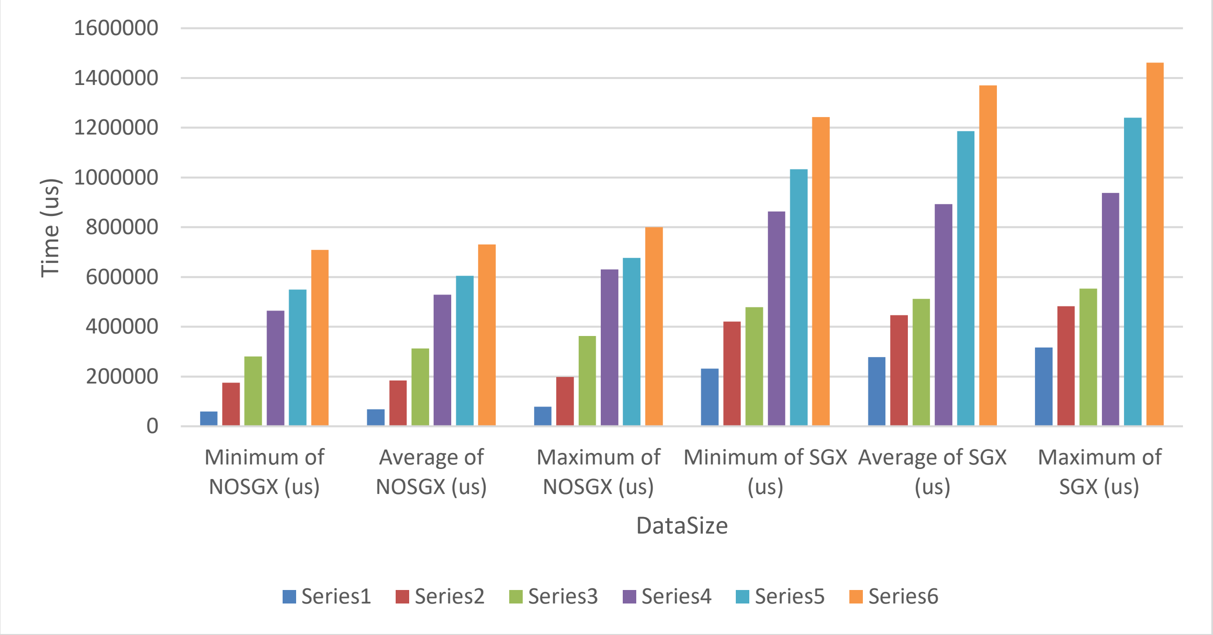

Figure 7: Representation of System Overhead Due to Various File Sizes

The overheads for NOSGX are 709,548us (minimum), 730,433us (average), and 800,180us (maximum) for a data size of 60kB, while SGX records greater overheads of 1,243,254us (lowest), 1,370,693us (average), and 1,461,046us (highest).

## VI. CONCLUSION

The trusted execution environment (TEE), an isolated, secure enclave within a computing platform, is at the centre of this project. TEEs have been harnessed by technologies like ARM's TrustZone and Intel's SGX, providing strong hardware-level mechanisms that separate the secure and nonsecure worlds.

Particularly Intel's SGX, which is expected to greatly improve e-Health security, has found relevance in situations like cloud computing and secure data aggregation.Blockchain technology has simultaneously become a crucial instrument in the fight for e-Health security. Blockchain-based smart contracts have proven to be adept at automating healthcare procedures while preserving data privacy and integrity. They offer clear and unchangeable records of medical transactions, paving the way for increased accountability.The holistic approach to e-Health security is further highlighted by a proposed system design. This architecture places an emphasis on user participation in data access control and includes users, medical research organisations, TEEs, blockchain, smart contracts, and storage servers. TEEs are essential to secure data processing, guaranteeing the confidentiality and integrity of sensitive healthcare data, while smart contracts transparently enforce access restrictions.Our comparison tests between SGX and non-SGX contexts highlight how useful hardware-level security is for e-Health. SGX has continually demonstrated the capacity to maintain the integrity and security of data, making it a potential option for the safe processing of medical data.

## REFERENCES

[1] Y. Chen, Z. Lu, H. Xiong, and W. Xu, “Privacy-preserving data aggregation protocol for fog computing-assisted vehicle-to-infrastructure scenario,” Security and Communication Networks, vol. 2018, pp. 1–14, 2018.

[2] L. Yang, W. Zou, and J. Wang, “EdgeShare: a blockchain-based edge data-sharing framework for industrial Internet of things,” vol. 43, 2021.

[3] F. Chen, J. Huang, C. Wang et al., “Data access control based on blockchain in medical cyber physical systems,” Security and Communication Networks, vol. 34, pp. 1–14, 2021.

[4] K. Gu, W. Jia, G. Wang, and S. Wen, “Efficient and secure attribute-based signature for monotone predicates,” ActaInformatica, vol. 54, no. 5, pp. 521–541, 2017.

[5] H.. Wang and Y.. Song, “Secure cloud-based EHR system using attribute-based cryptosystem and blockchain,” Journal of Medical Systems, vol. 42, no. 8, pp. 152–164, 2018.

[6] S. Ajani and M. Wanjari, "An Efficient Approach for Clustering Uncertain Data Mining Based on Hash Indexing and Voronoi Clustering," 2013 5th International Conference and Computational Intelligence and Communication Networks, 2013, pp. 486-490, doi: 10.1109/CICN.2013.106.

[7] Khetani, V., Gandhi, Y., Bhattacharya, S., Ajani, S. N., & Limkar, S. (2023). Cross-Domain Analysis of ML and DL: Evaluating their Impact in Diverse Domains. International Journal of Intelligent Systems and Applications in Engineering, 11(7s), 253–262. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2951

[8] R..Guo, H.. Shi, Q. Zhao, and D. Zheng, “Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems,” IEEE Access, vol. 6, pp. 11676–11686, 2018.

[9] J. S. Lee, C. J. Chew, and J. Y. Liu, “Medical blockchain: data sharing and privacy preserving of EHR based on smart contract,” vol. 74.

[10] R. Zou, X. Lv, and J. Zhao, “SPChain: blockchain-based medical data sharing and privacy-preserving eHealth system,” Information Processing & Management, vol. 58, no. 4, Article ID 102604, 2021.

[11] Z. Chen, W. Xu, B. Wang, and H. Yu, “A blockchain-based preserving and sharing system for medical data privacy,” Future Generation Computer Systems, vol. 124, pp. 338–350, 2021.

[12] A. Kosba, A. Miller, and E. Shi, “Hawk: the blockchain model of cryptography and privacy-preserving smart contracts,” in Proceedings of the 2016 IEEE Symposium on Security and Privacy, pp. 839–858, IEEE Press, Los Alamitos, CA, USA, 2016.

[13] P. Golle, K. Leytonbrown, and I. Mironov, “Incentives for sharing in peer-to-peer networks,” Lecture Notes in Computer Science, vol. 49, pp. 75–87, 2001.

[14] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, “Blockchain and federated learning for privacy-preserved data sharing in industrial IoT,” IEEE Transactions on Industrial Informatics, vol. 16, no. 6, pp. 4177–4186, 2020.

[15] X. Huang, Y. Lu, K. Zhang, S. Maharjan, and Y. Zhang, “Blockchain empowered asynchronous federated learning for secure data sharing in Internet of vehicles,” IEEE Transactions on Vehicular Technology, vol. 69, no. 4, pp. 4298–4311, 2020.

[16] A. A. Shrier, A. Chang, and N. Diakun-Thibault, Blockchain and Health IT: Algorithms, Privacy, and Data, 2016.

[17] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, “Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control,” Journal of Medical Systems, vol. 40, no. 10, p. 218, 2016.

[18] H. Li Hao, G. Xu, S. Liu, and H. Yang, “Towards efficient and privacy-preserving federated deep learning,” in Proceedings of the ICC 2019 - 2019 IEEE International Conference on Communications, pp. 1–6, ICC), Shanghai, China, May 2019.

[19] C. Priebe, K. Vaswani, and M. Costa, “EnclaveDB: A Secure Database Using SGX,” in Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP), IEEE, San Francisco, CA, USA, May 2018.

[20] R. Kunkel, D. L. Quoc, and F. Gregor, “TensorSCONE: a secure TensorFlow framework using intel SGX,” vol. 42, 2019.

[21] M. Abadi, P. Barham, and J. Chen, “TensorFlow: a system for large-scale machine learning,” USENIX Association, vol. 12, 2016.

[22] Q. Miao, H. Lin, J. Hu, and X. Wang, “An intelligent and privacy-enhanced data sharing strategy for blockchain-empowered Internet of Things,” Digital Communications and Networks, vol. 88, 2022.

[23] Kruse, C.S.; Mileski, M.; Vijaykumar, A.G.; Viswanathan, S.V.; Suskandla, U.; Chidambaram, Y. Impact of electronic health records on long-term care facilities: Systematic review. JMIR Med. Inform. IEEE 2017, 5, e35.

[24] Butpheng, C.; Yeh, K.-H.; Xiong, H. Security and Privacy in IoT-Cloud-Based e-Health Systems—A Comprehensive Review. Symmetry 2020, 12, 1191.

[25] Ismail, L.; Materwala, H. Blockchain Paradigm for Healthcare: Performance Evaluation. Symmetry 2020, 12, 1200.

[26] Malluhi, Q.; Tran, V.D.; Trinh, V.C. Decentralized Broadcast Encryption Schemes with Constant Size Ciphertext and Fast Decryption. Symmetry 2020, 12, 969.

[27] Hassen, O.A.; Abdulhussein, A.A.; Darwish, S.M.; Othman, Z.A.; Tiun, S.; Lotfy, Y.A. Towards a Secure Signature Scheme Based on Multimodal Biometric Technology: Application for IOT Blockchain Network. Symmetry 2020, 12, 1699.

[28] Abdulghani, H.A.; Nijdam, N.A.; Collen, A.; Konstantas, D. A Study on Security and Privacy Guidelines, Countermeasures, Threats: IoT Data at Rest Perspective. Symmetry 2019, 11, 774.

[29] Huh, J.-H. Big Data Analysis for Personalized Health Activities: Machine Learning Processing for Automatic Keyword Extraction Approach. Symmetry 2018, 10, 93. Kang, J.; Chung, H.; Lee, J.; Park, J.H. The Design and Analysis of a Secure Personal Healthcare System Based on Certificates. Symmetry 2016, 8, 129.

[30] Griebel, L.; Prokosch, H.-U.; Köpcke, F.; Toddenroth, D.; Christoph, J.; Leb, I.; Engel, I.; Sedlmayr, M. A scoping review of cloud computing in healthcare. BMC Med. Inform. Decis. Making 2015, 15, 17.

[31] Venčkauskas, A.; Štuikys, V.; Toldinas, J.; Jusas, N. A Model-Driven Framework to Develop Personalized Health Monitoring. Symmetry 2016, 8, 65.

[32] Chenthara, S.; Ahmed, K.; Wang, H.; Whittaker, F. Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing. IEEE Access 2019, 7, 74361–74382.

[33] Razaque, A.; Amsaad, F.; Khan, M.J.; Hariri, S.; Chen, S.; Siting, C.; Ji, X. Survey: Cybersecurity Vulnerabilities, Attacks and Solutions in the Medical Domain. IEEE Access 2019, 7, 168774–168797.

[34] Kim, J.W.; Edemacu, K.; Jang, B. MPPDS: Multilevel Privacy-Preserving Data Sharing in a Collaborative eHealth System. IEEE Access 2019, 7, 109910–109923.

[35] Bouras, M.A.; Lu, Q.; Zhang, F.; Wan, Y.; Zhang, T.; Ning, H. Distributed Ledger Technology for eHealth Identity Privacy: State of The Art and Future Perspective. Sensors 2020, 20, 483.

[36] Thatikonda, R., Padthe, A., Vaddadi, S. A., & Arnepalli, P. R. R. (2023). Effective Secure Data Agreement Approach-based cloud storage for a healthcare organization. International Journal of Smart Sensor and Adhoc Network, 60-70.

[37] Thatikonda, R., Vaddadi, S.A., Arnepalli, P.R.R. et al. Securing biomedical databases based on fuzzy method through blockchain technology. Soft Comput (2023). https://doi.org/10.1007/s00500-023-08355-x