

Towards Trustworthy Healthcare Systems: Designing Blockchain-Based Secure Electronic Health Records

Puneeta Singh¹, Shrddha Sagar²

¹Research Scholar, School of Computer Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh, India, puneeta12cs37@gmail.com

²Supervisor, School of Computer Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh, India, shrddha.sagar@galgotiasuniversity.edu.in

Abstract

Detecting fraudulent medical documents remains a significant challenge in the Web2 industry. This project proposes the use of blockchain technology and soul-bound tokens (SBTs) to automate and secure medical document verification. By leveraging deep learning and decentralized algorithms, this system aims to enhance the security, integrity, and accessibility of healthcare records. The goal is to provide seamless, real-time healthcare services while ensuring the confidentiality and security of sensitive health information. The current healthcare landscape is plagued by vulnerabilities in Electronic Health Records (EHRs), including security breaches, unauthorized access, and data manipulation. Existing methods for securing EHRs, such as encryption and access controls, have limitations in providing a comprehensive and tamper-proof solution. This research addresses critical challenges in data security, data integrity, interoperability, patient privacy, and scalability by designing a blockchain-based architecture for healthcare records. Blockchain technology offers an immutable and transparent ledger for medical records, enhancing the system's credibility and reducing the possibility of fraudulent activity. The proposed solution investigates the use of blockchain smart contracts to construct decentralized access control systems, enabling precise management of who has access to medical records. Additionally, the blockchain-based design takes healthcare data interoperability into account, facilitating trustworthy and easy data sharing between healthcare providers. The decentralized nature of blockchain can also lessen risks associated with centralized databases, enhancing the resilience of healthcare systems against cyber threats. The project prioritizes user empowerment, allowing patients to have more control over their electronic health records (EHRs) and enabling them to grant or revoke access as needed. The design also ensures compliance with current legal and ethical frameworks governing the management of electronic health records.

Keywords: Blockchain, SBT, Deep learning, NFT, IoT

1. Introduction

Although there are various well-established methods for confirming medical information, detecting changed or fraudulent papers remains a major challenge for the Web2 industry. There is an extreme requirement for cutting-edge automated technology. The actions and states of a deep learning system can be documented on

the blockchain. Since multiple agents can work together to learn and make decisions, this might pave the way for decentralized algorithms for reinforcement learning. Access to accurate, real-time healthcare services should be easy, smooth, and provided by a variety of features and services; this is the purpose of smart healthcare technology. The security and care with which these services deal with sensitive health information is of the utmost importance.

This token created by blockchain technology and can be transferred between users. When it comes to digital art and collectibles, NFTs are a great way to prove ownership. As an extension of NFTs, soulbound tokens (SBTs) aim to be linked to a specific individual or group and are not transferable. Just like other NFTs, SBTs can be publicly seen, and stored in an online wallet. There is no value in investing in SBTs. According to Weyl et al. (2022), they have the potential to represent the holder's affiliations, qualifications, commitments, and other attributes. Individuals can authenticate themselves using their authentic Web identities by utilizing SBTs provided by entities such as governments, businesses, and healthcare facilities. This allows other parties to easily and quickly verify this information without needing the issuer's help. Under investigation is a system that would allow any organization, be it a government agency, medical facility, or other entity, to issue soul-bound tokens as a means of verifying the legitimacy of reports, medical prescriptions, or any other kind of document.

Soul-bound tokens can be used to validate any individual's medical records because they are non-transferable and issued on the blockchain. As said earlier, Binance is the one that employs the technology of soul-bound tokens. In September 2022, Binance started offering its clients tokens that were connected to their accounts. Minting BAB is a breeze for Binance users after they've verified their identities. Using a combination of public and private data, SBTs may construct a user's social network. SBT attributes stand in for this data.

1.1.1 Soul-bound Tokens (SBT): The purpose of implementing SBT was to safeguard health records by preventing the exchange of sensitive medical information. The patient's private wallet and identity are the only things that SBTs are linked to, and they are non-transferable. To the owner of this token belongs full authority over their qualifications, reputation, and medical history.

1.1.2 Health Card Token (HCT): As a kind of ownership proof and medium of exchange, HCT is held by patients. Its construction guarantees security and uniqueness by adhering to the ERC721 standard for NFTs. The three positions that make up HCT are Owner (administration), Minters (doctors), and Users/Patients.

Some properties might be accessible only to authorized users due to their encryption, while others could be open to everybody. This means the data that the SBT issuer wants to disseminate via SBTs is entirely up to them. Below, you will find the Tokens shown in Figure 1:

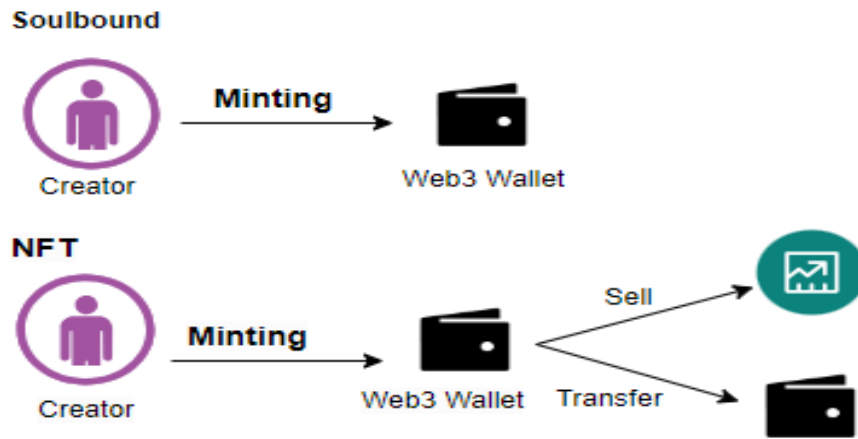


Figure 1: Representation of SBT vs NFT

1.2. Problem Statement

In the current healthcare landscape, Electronic Health Records (EHRs) are vulnerable to security breaches, unauthorized access, and data manipulation. Instances of data breaches and cyber-attacks have raised serious concerns. The existing methods for securing EHRs, such as encryption and access controls, have limitations in providing a comprehensive and tamper-proof solution. There is a critical need for a robust, transparent, and decentralized system.

This research aims to address the following challenges:

- ❖ **Data Security:** Develop a Blockchain-based architecture that ensures the security and confidentiality of patient records, protecting them from unauthorized access and cyber threats.
- ❖ **Data Integrity:** Design mechanisms to guarantee the immutability and integrity of healthcare records, preventing unauthorized modifications and ensuring the accuracy of patient information.
- ❖ **Interoperability:** Create a standardized and interoperable Blockchain solution that can seamlessly integrate with existing healthcare systems, fostering collaboration and data exchange among different entities in the healthcare ecosystem.
- ❖ **Patient Privacy:** Implement privacy-preserving features to empower patients with control over their own health data, adhering to regulatory requirements and ethical standards.
- ❖ **Scalability:** Address the scalability challenges associated with Blockchain technology to ensure its feasibility for large-scale healthcare systems, accommodating the growing volume of electronic health data.

1.3. Significance of Research:

Blockchain technology guarantees an unchangeable and transparent ledger for medical records. By offering a tamper-resistant and auditable history of patient data, enhances the system's credibility by lowering the possibility of fraudulent activity.

- ❖ **Uncentralized Access Management:** The study investigates the use of blockchain smart contracts to construct decentralized access control systems. This method enables precise management of who has access to medical records.
- ❖ **Data Integrity and Interoperability:** The blockchain-based system's design takes healthcare data interoperability into account. The project intends to establish a system that facilitates trustworthy and easy data sharing between healthcare providers by using standardized protocols and the blockchain's consensus mechanism to ensure data integrity.
- ❖ **Adaptability to Cyberthreats:** The study investigates how the decentralized nature of blockchain can lessen risks associated with centralized databases, hence enhancing the resilience of healthcare systems against cyber assaults. This covers defence against data manipulation, ransomware assaults, and other nefarious activities.
- ❖ **Ownership and Empowerment of Users:** Ownership of health data and user empowerment are prioritized in the proposed system. Patients can have more control over their electronic health records (EHRs) by using blockchain technology, allowing or removing access as needed. This helps to make healthcare record management more patient centric.
- ❖ **Optimizing performance and scalability:** It investigates novel ways to maximize system performance without sacrificing security.
- ❖ **Adherence to Regulations:** The design ensures that the suggested blockchain-based solution complies with current legal and ethical frameworks governing the management of electronic health records by considering compliance with healthcare regulatory requirements.

"Towards Trustworthy Healthcare Systems: Designing Blockchain-Based Secure Electronic Health Records" is a research contribution that seeks to further the state of healthcare data security by offering a framework for the development of patient-centered, transparent, and safe electronic health record systems.

2. Literature Review:

Blockchain technology's data sharing, decentralization, and security benefits are examined, as well as its potential applications in business, e-government, smart governance, and healthcare. The report also discusses the limitations of traditional record-keeping and how blockchain technology may help. Blockchain technology is being studied in healthcare to improve data integrity, classify medical pictures, anticipate diseases, and stop drug counterfeiting in supply chain management. The article also discusses Soul bound tokens, which are digital tokens that can verify a person's identity or ownership of an item. Soul bound tokens can replace

centralized digital document verification. The literature analysis provides a solid foundation for the research study and highlights how deep learning and blockchain technology might improve medical document verification efficiency, security, and accuracy. Blockchain technology aims to create a decentralized, unsupervised system (Yli-Huumo et al., 2016). It is used in business, e-government, smart government, and healthcare due to its benefits (Sidhu, 2017, pp. 1-6; Hou, 2017, pp. 1-4; Arendsen et al., 2011). Deep learning, which can be learned from data, is based on artificial neural networks and is utilized in cybersecurity, text analytics, healthcare, and image identification. Blockchain can offer safe and accurate results. Machine learning requires enough reliable data. They studied blockchain technology for cloud computing security and trust. The study seeks to investigate how blockchain technology might create a distributed and decentralized trust architecture that improves cloud transaction integrity and traceability. Traditional record-keeping requires large storage facilities and can be difficult to obtain documents. The public cannot access these medical records. Medical records should be available to patients or authorized caretakers. Jamil et al. (2019) studied how blockchain technology might prevent drug counterfeiting in supply chain management. This innovative blockchain system captures the safe and transparent transit and handling of drugs from producer to patient, improving drug supply chain efficacy and safety. Umamaheswaran et al. polled 150 machine learning and blockchain experts in medicine to explore their healthcare applications (2022). Medical picture categorization, disease prediction, and blockchain data integrity improved in the study. BinDaaS (Bhattacharya et al., 2019, pp. 1242-1255) uses deep learning algorithms and blockchain technology to share EHR between several healthcare providers. A public blockchain allows anybody to join and verify Soul bound tokens.

Since anybody may verify digital papers, this system is more transparent and decentralized. It may be less secure because it relies on network security rather than a more restricted group of entities. They showed a multi-chain application that covers inclusive governance, asset recovery, data integrity, and identity security in decentralized networks. They want to offer under-collateralized lending so borrowers can get loans while retaining a trustworthy web presence. The NFT ecosystem relies on non-fungible token marketplaces (NFTM), which pose security vulnerabilities. Das et al. presented NFT exchange on NFTM Dapp platforms in 2021. The process is full of security risks. They discussed the potential that Open Sea and Rarible NFTs are fake. When an NFT is advertised, the NFTM seizes the token, allowing the seller to sell it to the buyer. To do this, the NFTM must own, own, or operate the NFT. The escrow model is risky because all platform assets are housed in a single NFTM-managed escrow contract or wallet.

The security of the escrow contract or the external account that controls it determines the security of all marketplace assets (Das et al., 2021). Verifiable credentials (VCs) and decentralized identifiers (DIDs), the technology used to create digital identities, are not standardized, allowing user data leakage and composability issues. A negative reputation and irreversible "scarlet letter" consequences now threaten users. SBTs, however, are still being defined and may offer additional protection and resilience to these threats (Jain et al., 2022).

A University of Nicosia (2018) tool makes and stores bitcoin certificates. Additionally, UNIC accepts bitcoin

for degree programs. This technique may cost platform users because it requires keeping large volumes of data and documents, such as transcripts, diplomas, and certificates. This research examines SBTs to overcome the difficulties with the present NFT methodology. Soul bound tokens (Weyl et al., 2022) have been extensively studied and may improve digital document security and verifiability.

Identifying research gaps in the context of a Blockchain framework for ensuring security in healthcare records involves assessing the existing literature and pinpointing areas where further investigation is needed. Below are some potential research gaps in this domain:

1. **Integration with Existing Healthcare Systems:** Limited studies address the seamless integration of Blockchain solutions with existing healthcare information systems. Further exploration is needed to understand the challenges, strategies, and best practices for integrating Blockchain into diverse healthcare infrastructures.
2. **Scalability and Performance Optimization:** Existing studies may not adequately address the scalability issues associated. Research is needed to explore scalable solutions and performance optimization techniques to ensure efficient processing and storage.
3. **User Acceptance and Usability:** Limited attention may have been given to user perspectives, including healthcare professionals, administrators, and patients, regarding the acceptance and usability of Blockchain-based healthcare record systems. More research is needed to understand user concerns, preferences, and barriers to adoption.
4. **Interoperability Standards:** Interoperability standards for Blockchain-based healthcare systems may not be well-established. Investigating and proposing standardized protocols for data exchange and communication between different healthcare entities using Blockchain technology is a crucial research gap.
5. **Regulatory Compliance and Legal Implications:** The legal and regulatory aspects of implementing Blockchain in healthcare records need further exploration. Understanding how Blockchain complies with healthcare data protection regulations and addressing legal challenges associated with decentralized systems is an important research area.
6. **Privacy-Preserving Techniques:** Enhancing privacy in Blockchain-based healthcare records without compromising security is a challenging area. Investigating advanced cryptographic techniques or privacy-preserving protocols specific to healthcare data is essential for filling this gap.
7. **Blockchain Consensus Mechanisms in Healthcare:** While various Blockchain consensus mechanisms exist, their suitability and effectiveness in healthcare settings may not have been thoroughly studied. Research is needed to evaluate and recommend consensus mechanisms tailored to the requirements and constraints of healthcare data.
8. **Cost-Benefit Analysis and ROI:** Limited research may have explored the cost-effectiveness and return on investment (ROI) of implementing Blockchain in healthcare records. Investigating the economic viability and long-term benefits of adopting Blockchain is crucial for decision-makers in the healthcare industry.

9. **Blockchain Security Threats and Countermeasures:** Ongoing advancements in cybersecurity may introduce new threats to Blockchain-based healthcare systems. Research is needed to identify emerging security threats and develop effective countermeasures to protect sensitive healthcare data stored on the Blockchain.
10. **Educational Initiatives and Training:** empower healthcare professionals with the knowledge and skills required for interacting with Blockchain-based systems. Research could explore effective training methods and educational strategies in this context.

These research gaps provide a foundation for scholars and researchers to contribute valuable insights and advancements in the field of Blockchain for securing healthcare records.

2.1 Motivation and Objectives

This study's main goal is to carry out energy-efficient health monitoring that is fast and secure. A patient's remote healthcare monitoring system design in WBAN posed several difficulties [27]. Because it is accomplished either intra-WBAN or outside WBAN, current WBAN systems do not provide end-to-end security, low energy consumption, and can create delays. The interference between WBANs occurs when they use the same channel at the same time. Periodical data requires the optimum channel for interference-free transmission, while vital data requires an idle channel. High energy usage and end-to-end latency are brought on by single-hop communication for the crucial data. To transmit packets by QoS restrictions, the contention window size (CWS) at the single hop must be modified. None of them gave environmental information about a patient's health any thought. The following health monitoring-related challenges, of which the principal ones are enumerated below, serve as our driving force.

Higher energy consumption: Frequent sensor replacement is necessary when sensors exhaust their energy.

Data security and privacy are compromised by wireless channels and the limited energy capacity of sensors.

Mobility forecast: While a patient is moving around, communications must be secure and energy-efficient.

The following list of research goals is included in this paper:

- To put out a health monitoring system that enables patients to perceive and send data in an energy-efficient manner while still being secure and delay-aware.
- To maintain QoS restrictions while gathering and sending data from all tiers (intra-WBAN, inter-WBAN, and beyond WBAN).
- Ensuring the integrity and confidentiality of the data is maintained while securely storing the sensed data on a storage server.

2.2 Key Elements of Blockchain Technology:

- **Decentralized:** Blockchain operates without a central authority, allowing global data recording, storage, and modification without the need for centralized control nodes.
- **Transparent:** Trust is established through transparency. All data stored in the blockchain is accessible to every node, ensuring that participants can access the most recent and reliable information.
- **Open Source:** Most blockchain systems are public and open source. This transparency enables anyone to review the records and encourages the development of applications by leveraging blockchain technology.
- **Autonomy:** Blockchain aims to shift control from individual entities to the entire system. This is achieved through consensus mechanisms, ensuring each node on the network can securely transfer or modify data.
- **Immutable:** Records in the blockchain are permanent and tamper-proof. The use of cryptographic hashes and the requirement of controlling more than 51% of the nodes simultaneously make it extremely difficult to alter recorded information.

2.3 Healthcare Management:

- **Concerns in EHR Management:** Despite the benefits of EHRs, concerns persist regarding data ownership and security within these systems.
- **Prominent Blockchain Platforms:** Ethereum and Hyperledger are popular choices for implementing blockchain in healthcare. Their permissioned networks and efficient transaction processing make them suitable for managing sensitive health data.
- **Global Initiatives:** Governments worldwide recognize the importance of digitizing medical systems. Initiatives like the HITECH Act promote widespread EHR use for societal benefits, emphasizing streamlined administration and enhanced data sharing.
- **Crisis Management and EHRs:** Events like the 2019 novel coronavirus outbreak highlight the crucial role of EHRs in crisis management. Blockchain showcases its potential in telemonitoring and healthcare technologies during such events.

2.4 Using soulbound tokens and pseudo code, medical document verification on the blockchain

Start: SBT_Enabled_Hospital (Step 1)

Start the blockchain from scratch and make a fresh soulbound token contract.

2. Confirm which hospitals are authorized to provide SBTs.
3. Establish a user interface so that papers may be uploaded and verified.
4. Figure 2 shows the logic of verification of institutions allowed to mint SBTs as below.

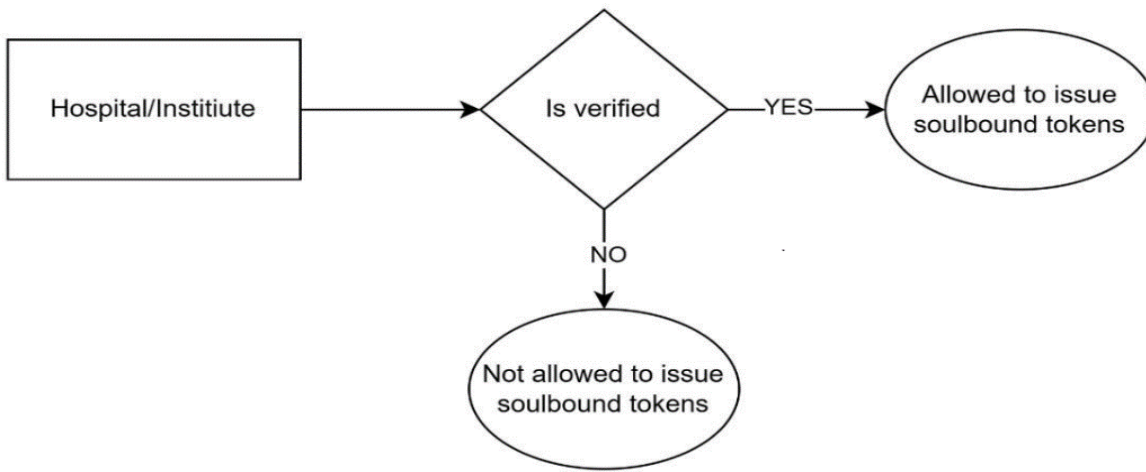


Figure 2: Verification of institutions allowed to mint SBTs

SBT_Enabled_Document in Step 2

Section A: Process of uploading documents:

Digital document input

Result: Soulbound token Method:

1. The document is uploaded to the interface by the hospital.
2. The document is hashed and placed as a soulbound token on the blockchain.
3. The user's identity is connected to the soulbound token.



Figure 3: Hospital issuing SBTs

In Figure 3, the patients at the accredited hospitals and facilities may receive fresh SBTs. These SBTs include the URL for the document's decentralized network hosting—which takes the form of a prescription or report.

Part B:

To create a digital medical record

Input soulbound tokens.

Output: Soulbound token hash

Step 1: Access the user's address and obtain a medical record.

2. Users' soulbound token ownership is validated.
3. The soulbound tokens are hashed using the SHA256 technique after verification.

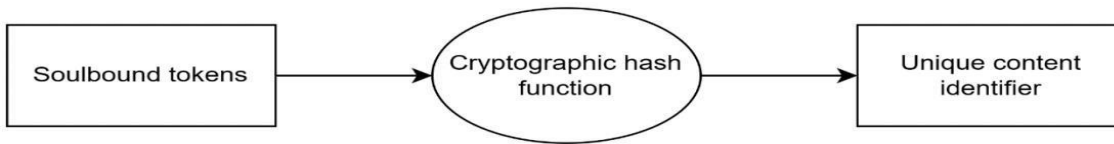


Figure 4: Generation of a hash of soulbound tokens on IPFS.

Figure 4 demonstrates the phase of generation of a hash of soulbound tokens on IPFS.

Step 3: Document Verification with SBT Enabled

Enter: URL of digital health record Output: Verified or unverified document Method:

1. The user authenticates himself to the verification system by presenting their medical record.
2. The soulbound tokens connected to the displayed record are retrieved by the system.
3. The system verifies the connection between the user's identity and the soulbound token.
4. The document is validated, and the verification is noted on the blockchain if the connection is legitimate.
5. The verification request is denied if the link is not legitimate.

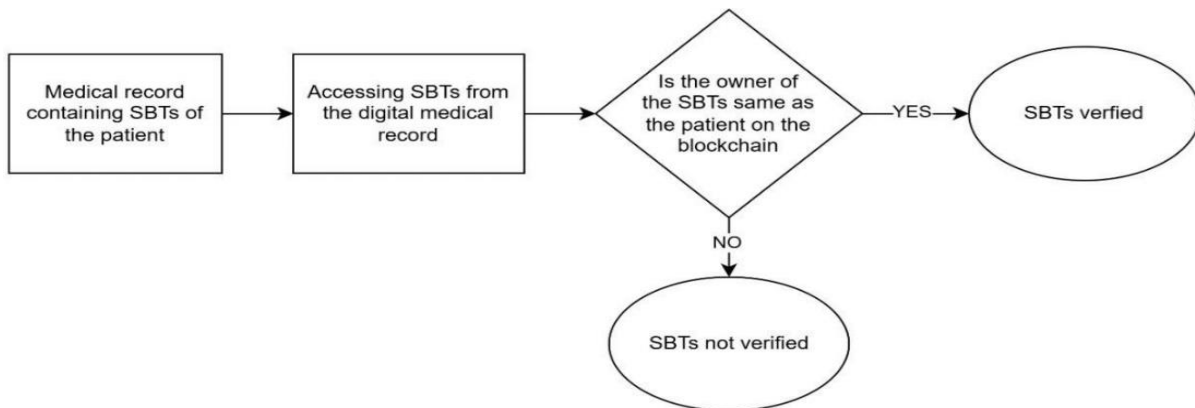


Figure 5: Verification of medical record using SBTs.

In figure 5, the digital medical record can be verified by utilizing the hospital's token ID and smart contract address to get the owner of the SBTs included in the record from the blockchain. It is verified that the patient's address matches the SBT owner's after gaining access to the SBT owner. The SBTs are validated if the owners are the same shown in figure 6 as below.

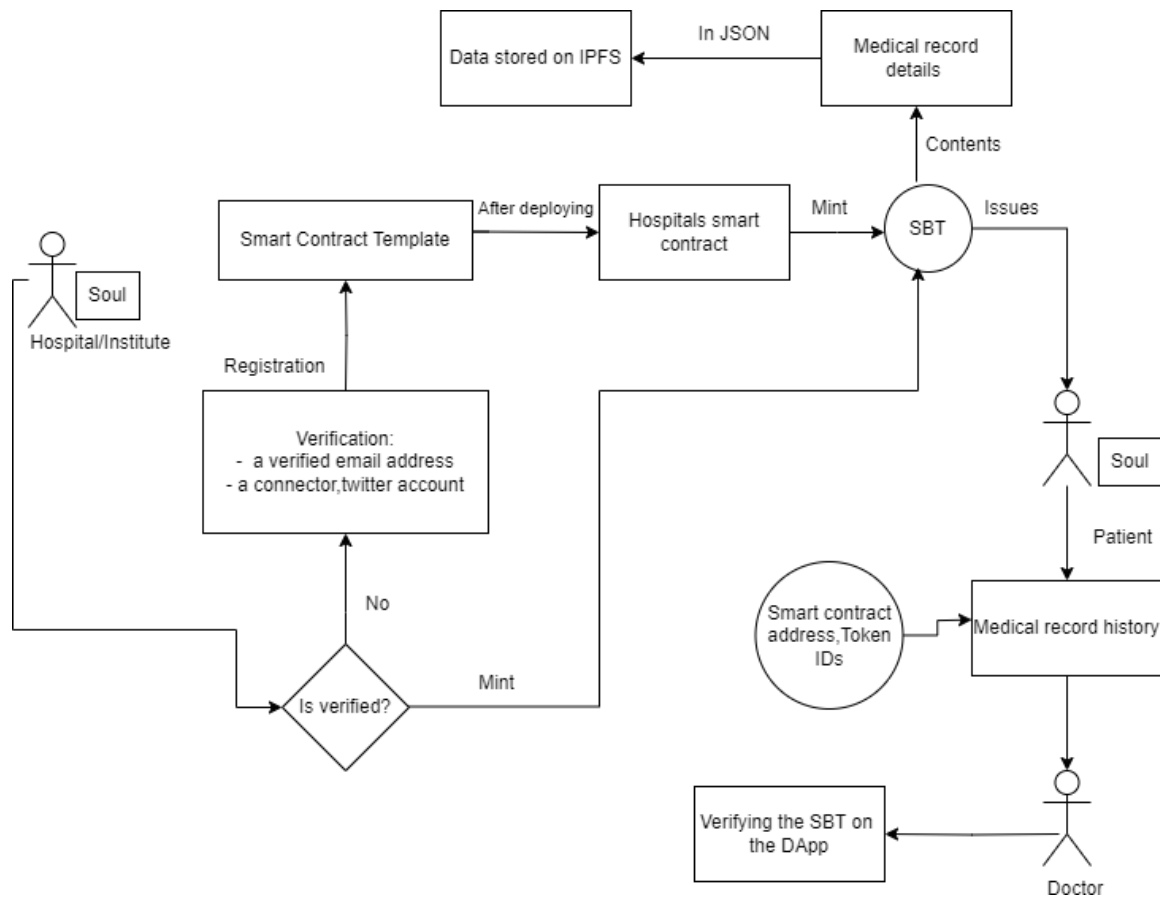


Figure 6: Flowchart of Document Verification SBT

3. METHODOLOGY/ SYSTEM MODEL

The blockchain-based soulbound token system for credential issuance, verification, and recovery is suggested as a solution. With selective disclosure, this system gives users total control over credential information. The credentials are distributed in the form of NFT on the blockchain, and the NFT data is encrypted and saved on the IPFS (Interplanetary File System).

3.1 System Model

Three entities are involved in the implementation of the suggested solution: the issuer entity, the verifier, and the user (holder). The agency that oversees and distributes the SBT to the user may be any reputable agency or government division. The user is a regular person who contacts the organization to request the issuance of credentials. People or organizations seeking to verify credentials can act as the verifier. The credential issuance and recovery process's system architecture is shown in figure 7 as follows:

In Figure .7. Depicts a user registration to register with the system providing the necessary information and the system verifies the information and creates a user profile. In credential Issuance, the system generates a

unique credential (e.g. username/password, token, certificate).

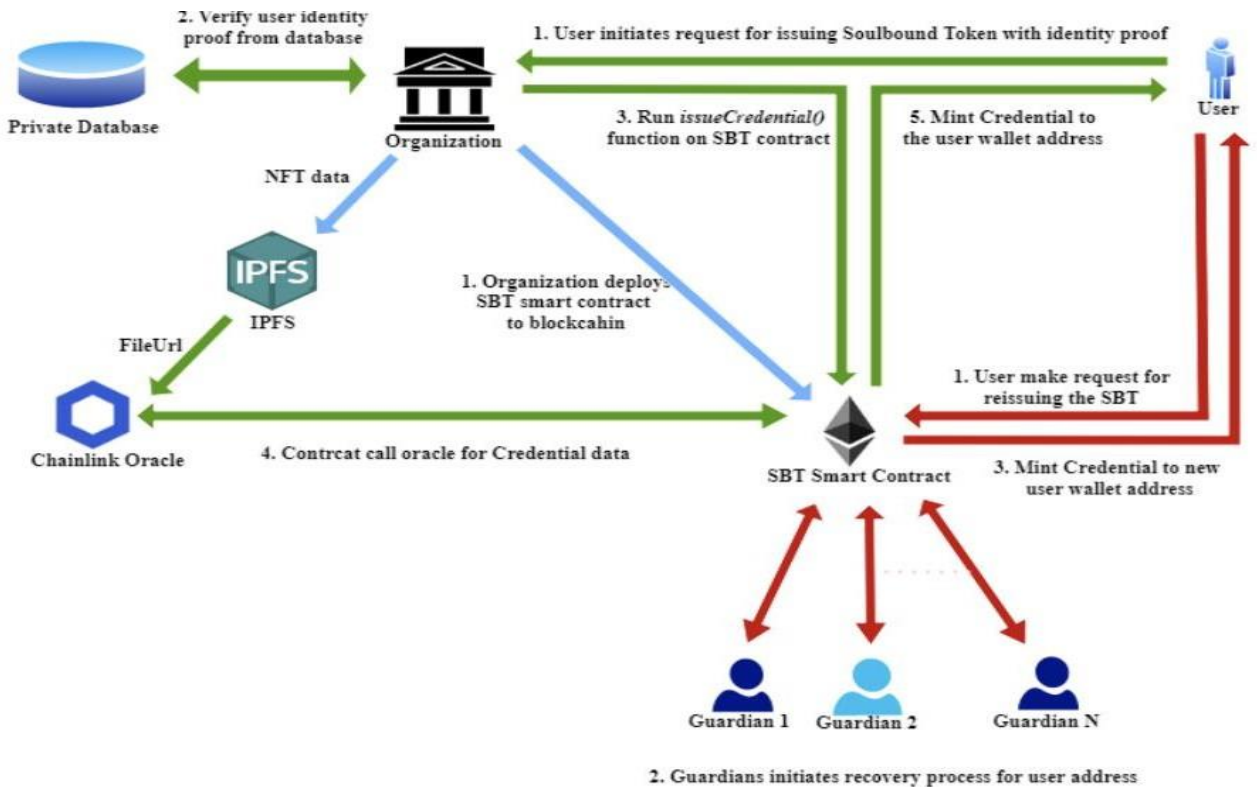


Figure 7: System design for the process of issuing credentials and recovering them.

In Figure .7. Depicts a user registration to register with the system providing the necessary information and the system verifies the information and creates a user profile. In credential Issuance, the system generates a unique credential (e.g. username/password, token, certificate).

3.1.1. Deploying contract

The SBT contract is published by the issuing organization on the blockchain, which is accessible by any business.

3.2. Issuing of credential

The request to issue the credential is made by the user. The user provides the organization with their identity, wallet address, and guardians' address. The company then confirms the user identity data and looks up legitimate guardian addresses, which can't be repeated. The organization executes the `issueCredential()` method on the SBT contract when the data has been satisfactorily verified. These are the stages that the `issueCredential()` method takes to operate.

Credential characteristics are generated via the off-chain function and encrypted using the user's public key. The off-chain function creates the encrypted credential and uploads it to IPFS depicted in figures 8-10.

In Figure 8. Representation of the soulbound token where to design the program flow for issuing the soul-bound token credential to both the user and the organization. The user registers with the system, providing necessary information (e.g. name, email, organization). In organization registration, the organization registers with the system, providing necessary information (e.g. name, contact, information, etc.)

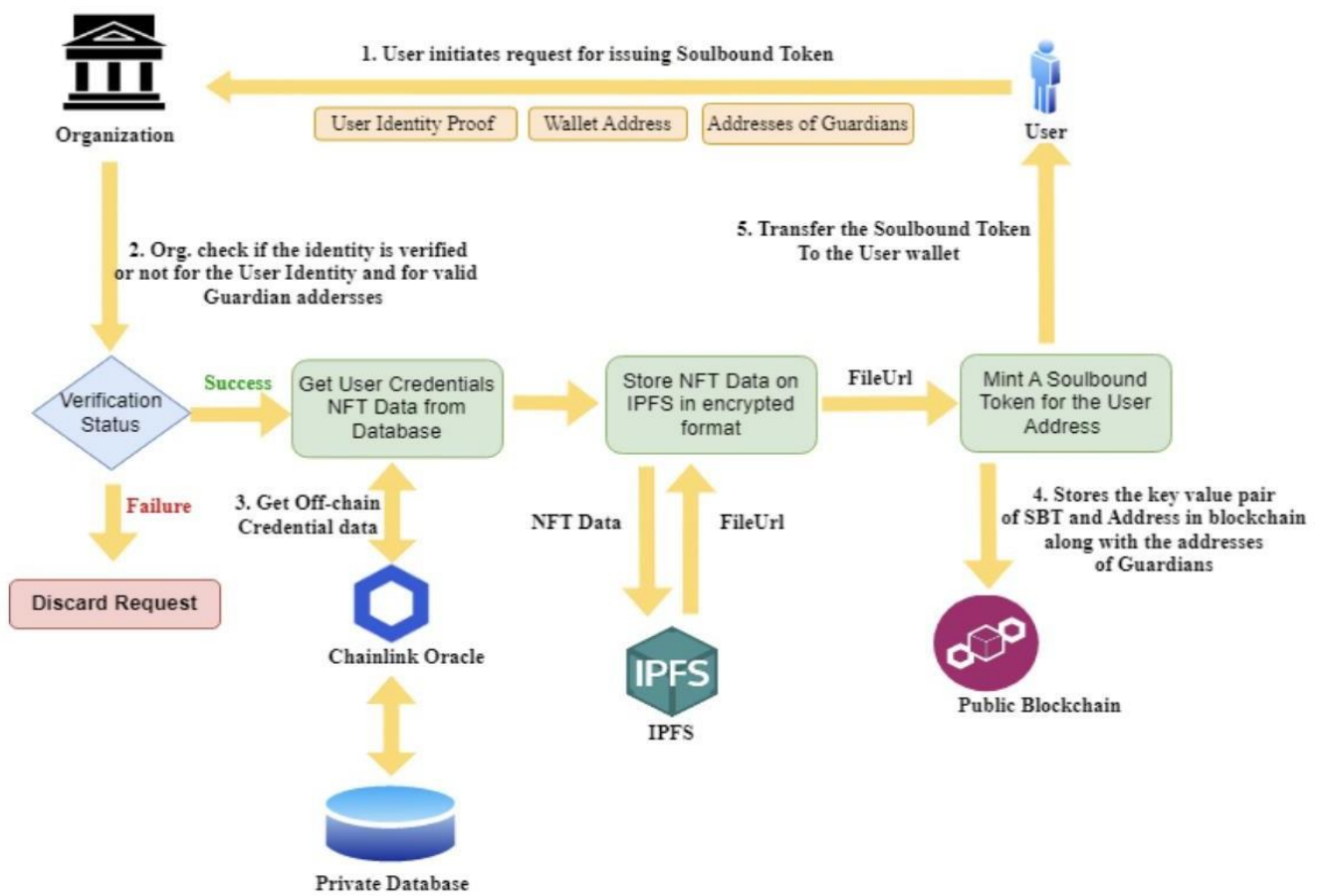


Figure 8: Program flow for issuing the soulbound token credential to the user and the organization.

Figure 9 shows selective credential disclosure allows users to share only the necessary information from their credentials with different verifiers, maintaining privacy and security. In this user requests verification, the verifier requests credentials, user selects credentials and verifier credentials.

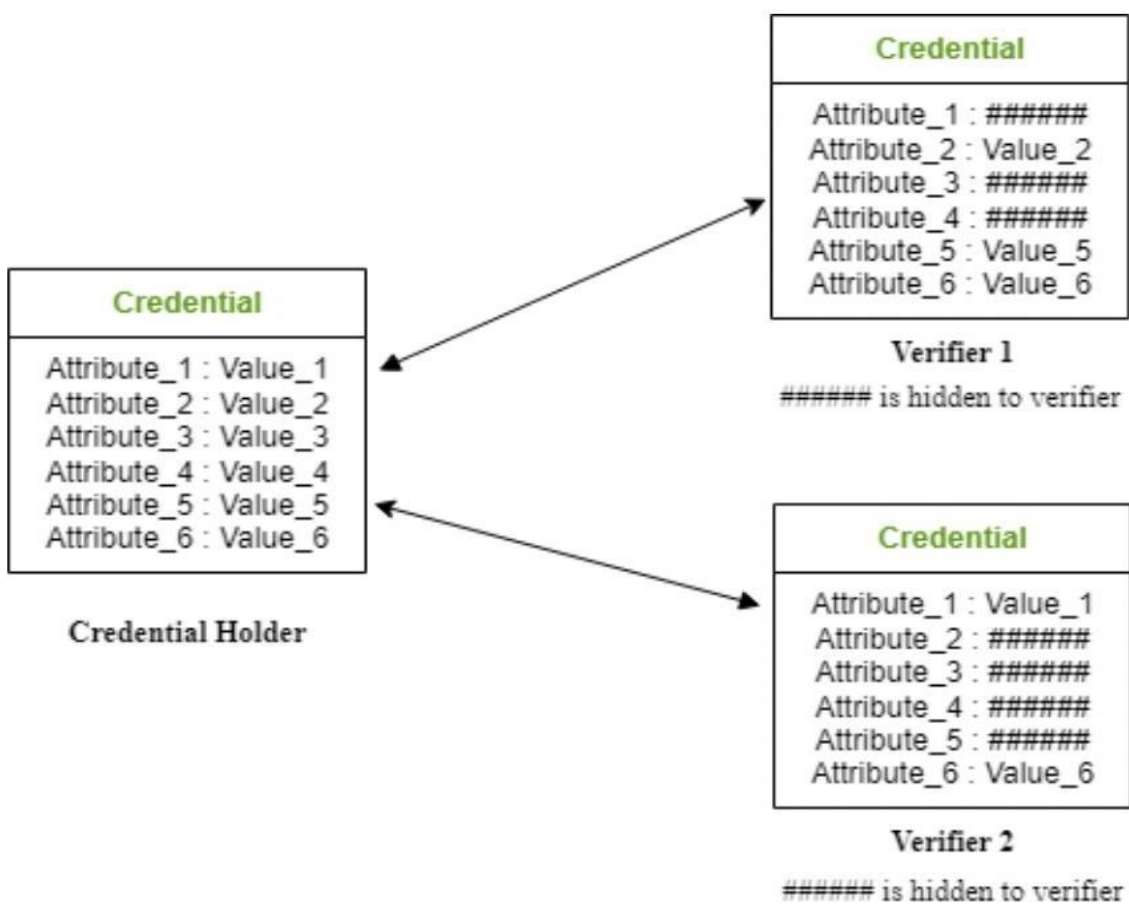


Figure 9: selective credential disclosure for various verifiers.

Figure 10 shows user requests verification where the user initiates a request to verify their soul-bound token credential with a verifier. The verifier requests the user to present their soul-bound token credential.

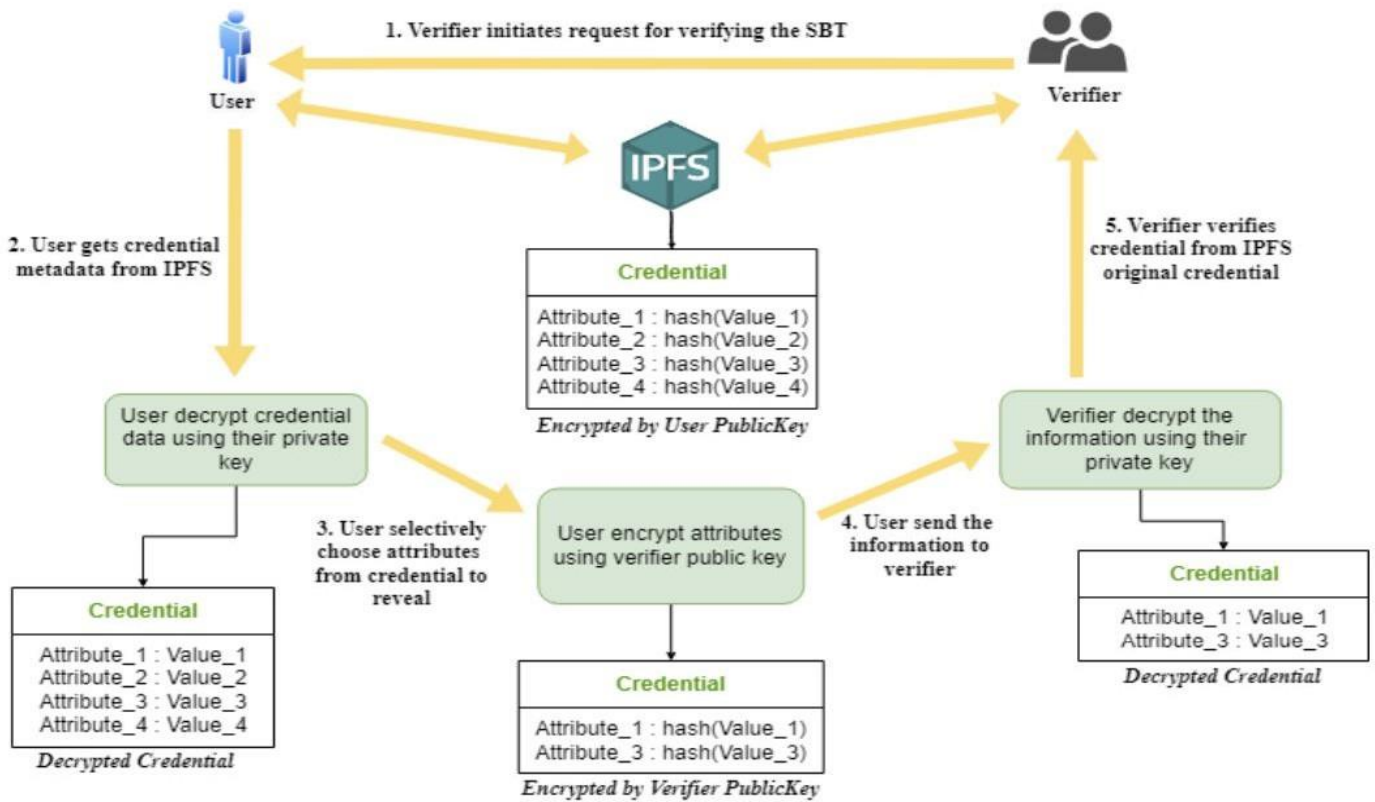


Figure 10: Program flow between the user and the verifier to confirm the credential for the soulbound token.

3.3. Verification of credentials:

This method selectively discloses credentials to the verifier. The credential holder decides what to show the verifier. Figure 3 shows selective credential sharing to several verifiers. The verifier requests the holder's SBT credential to commence verification. It is unlocked with their private key, so only they can read it. Holders can divulge attributes to verifiers only. Holder decrypts credential properties with private key. The holder encrypts it with the verifier's public key and sends it to them. Verifiers decrypt holder data. The holder verifier verifies credential authenticity in Figure 4.

3.4. Recovery Process for SBT

The user enters the new wallet address when calling `reissueCredential()`. Guardians must retrieve credentials using SBT contract's `initiateRecovery()` function. If the function is invoked more than the minimal number of times, `executeRecovery()` is called. The old SBT will be burnt and the new SBT issued to the new user wallet address in figure 11.

Figure 11 shows a generalized program flow for reissuing a “soul-bound token credential” between a user and an organization. User request re-issuance which the user initiates a request to reissue their soul-bound token credential. This request can be made through a user interface or an API. The organization verifies the request, revocation of previous credentials, binding new credentials, and delivery of new credentials.

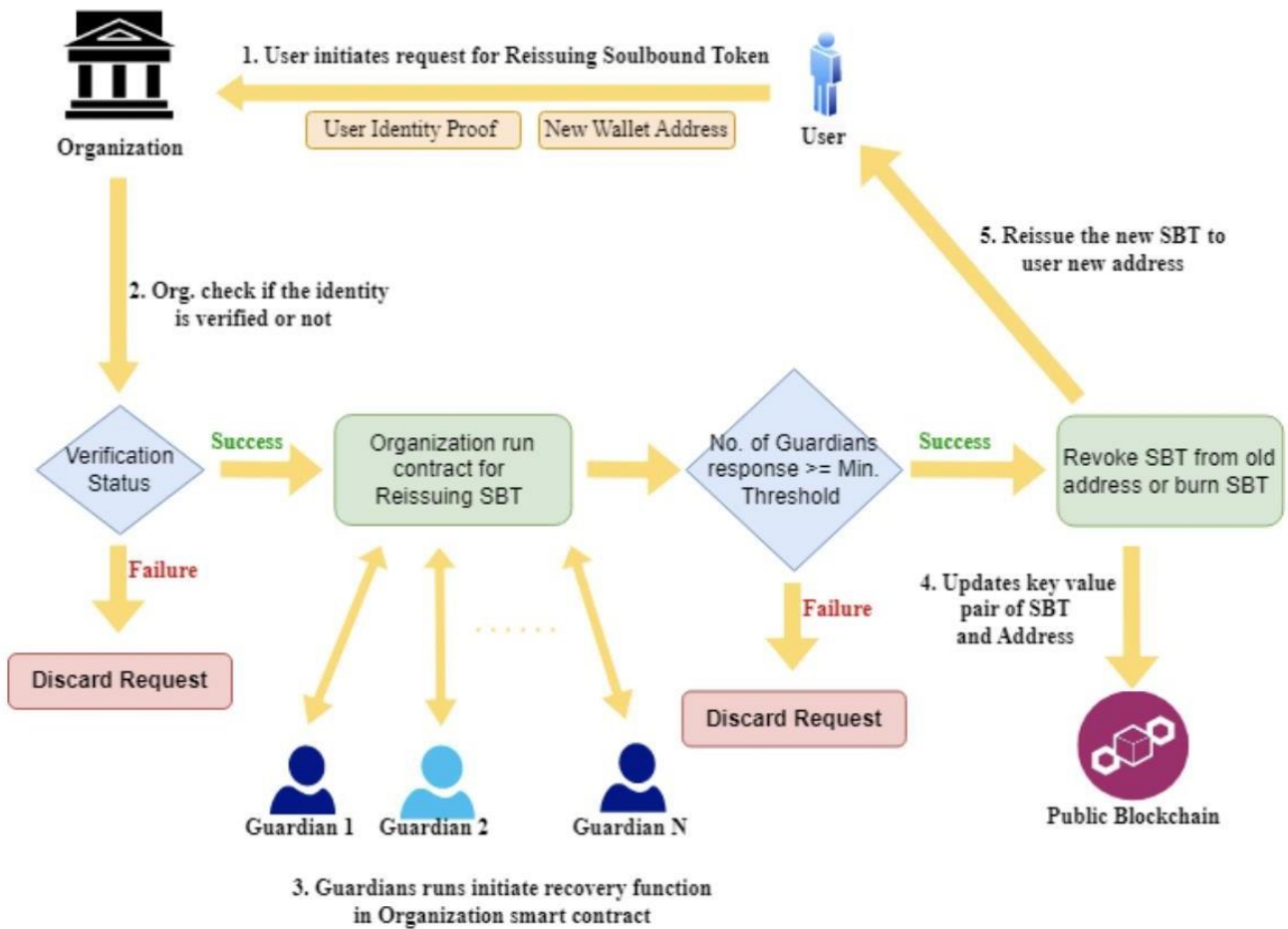


Figure 11: Program flow for reissuing the soulbound token credential between the user and the organization

3.5. Smart contract:

One smart contract credential (SBT) is used in this scheme. Solidity is the language used in this smart contract. Once the organization verifies the user identification off-chain, the function `initiateCredentialRequest()` is executed. This accepts as input an array of guardian addresses and the user address. The addresses that wish to take on the role of guardian for the user address are known as guardian addresses. This function runs the `issueCredential()` function after verifying that guardian addresses are legitimate.

The guardian addresses hash is added to the appropriate mapping with the user address by this `addGuardian()` function, which accepts as inputs the user address and their corresponding guardian addresses array. It looks for guardian address duplication before adding to the mapping. The user address was entered into the `issueCredential()` method, which is used to issue the SBT credential to the user address. Multiple function calls are used by this function. It starts by using the `getCredentialUrl()` function, which uses a chain-link oracle to search the organization's private database for the credential and connect to an off-chain API. Using the user's public key, this API encrypts the credential characteristics before uploading them to the IPFS. The `issueCredential()` function receives the produced file URL back. It invokes the `safeMintCredential()` method to mint the soulbound token for the token URL and assign it to the user address after receiving the credential file URL from the function. Finally, it stores the `tokenId` in the `addressToSBT` mapping associated with that user address shown in figure 12.

Credential SBT.sol
<pre>+ SBT Details : struct{uint issued, uint256} + addressToSBT : mapping(address => SBTDetails) + addressToGuardianAddresses : mapping(address => address[]) + RECOVERY_THRESHOLD : uint256 constant + addressToRecoveryGuardians : mapping(address => address[])</pre>
<pre>+ initiateCredentialRequest() : external + issueCredential() : onlyOwner + addGuardian() : onlyOwner + safeMintCredential() : onlyOwner + generateCredentialUri() : onlyOwner + revoke(): public + initiateRecovery() : external + cancelRecovery() : external + executeRecovery() : external</pre>

Figure 12: Program flow in Smart Contract Credential (SBT)

Revoke() deletes the user's tokenId. Reissuing the SBT via the recovery method activates this function. The initiate recovery() function lets a guardian start user recovery.

Complete algorithm: SBT-based Document-Verification

1. SBT_Enabled_Hospital is contacted for hospital verification in order to register and authenticate an institution or hospital.

$$H + SBi = H\#$$

i) H = Hospital

ii) SBi => ID of Hospital

iii) H# => Smart contract for the hospital

2. Hospitals may call SBT_Enabled_Document to obtain fresh prescriptions or reports in the form of SBTs for their patients following a successful verification process.

$$H\# \otimes SBT(i,j)$$

i) Soulbound token => SBT

ii) i => Accredited medical facility

iii) j => Token ID

3. By generating a cryptographic hash of their soulbound tokens, which are kept on IPFS, each patient can create their own digital medical record.

$$x \ n \ SBT \ (i,j) \ \blacktriangleright \ Document$$

i) n => Total SBTs

ii) Docu => IPFS medical record

4. The medical record link must be entered in order to invoke SBT_Enabled_Document_Verification, which will automatically confirm the SBTs granted to that patient. This process can be repeated for any SBT-enabled document.

$$Document \ \otimes \ Address(Patient) == Owner(SBT \ (i,j))? \ \otimes \ Confirmed$$

i) Owner(SBT) => SBT owners in the electronic medical record

ii) Address(Patient) => The patient's wallet address

3.6. Performance Analysis:

The method of assessing the suggested algorithm's efficacy and efficiency is investigated. Examining the suggested system and comparing its total man-hours spent verifying to the available manual approaches, it is established how it differs from them. To assess the overall effectiveness of the suggested system, a number of measuring criteria are used, including the amount of time required for verification, spending, authentication, security, and automation.

3.6.1. Time:

The intricacy can all have a significant impact on how long it takes to verify a medical document. A medical document's complete verification generally takes a few days to several weeks. The reading data stored by SBT from a blockchain can be done rather quickly. In Polygon, adding a block typically takes 2.2 seconds on average.

3.6.2. Security and Authentication:

The following are some of the reasons that make having SBTs for medical records unnecessary:

- **Immutability:** Data cannot be changed or removed from a blockchain once it has been recorded there. This makes it more difficult for someone to alter the data or create false records or documents.
- **Decentralization:** Because blockchains are dispersed among several computers, or nodes, they are decentralized, making it difficult for one person to manage the data or make changes to it without the network's consent.
- **Cryptographic hashing:** By putting some data through a mathematical procedure, cryptographic hashing creates a distinct "hash" that serves as a representation of the original material. Without disclosing the actual substance of the data, this hash can be used to confirm their legitimacy.
- **Consensus algorithms:** Before a transaction is put to the blockchain using these techniques, several nodes on the network must agree on its validity.

3.6.3. Automation:

Prescriptions, reports, and other medical records need to be verified. This is a laborious process that is not automated at the moment. Prior to validating a particular document, the patient must first be validated using their social security number, medical record number, allocated identification number, etc. A patient who possesses soulbound tokens can use them to build a hash of other soulbound tokens. All of the information on the patient's prescriptions and medical reports is contained in this hash. By providing the hospital or institution with this one hash, which includes information about all of the patient's soulbound tokens.

4. Results:

Soulbound tokens may be able to offer a tamper-proof record of a document's legitimacy in the context of document verification. This would give rise to an unchangeable and safe record of the document's issuance that anybody with blockchain access could confirm shown in figures 13-17.

Figure 13 shows the representation of document verification can vary depending on the context and the specific requirements of the system(document submission, document validation, data extraction, verification, decision, notification and their record keeping).

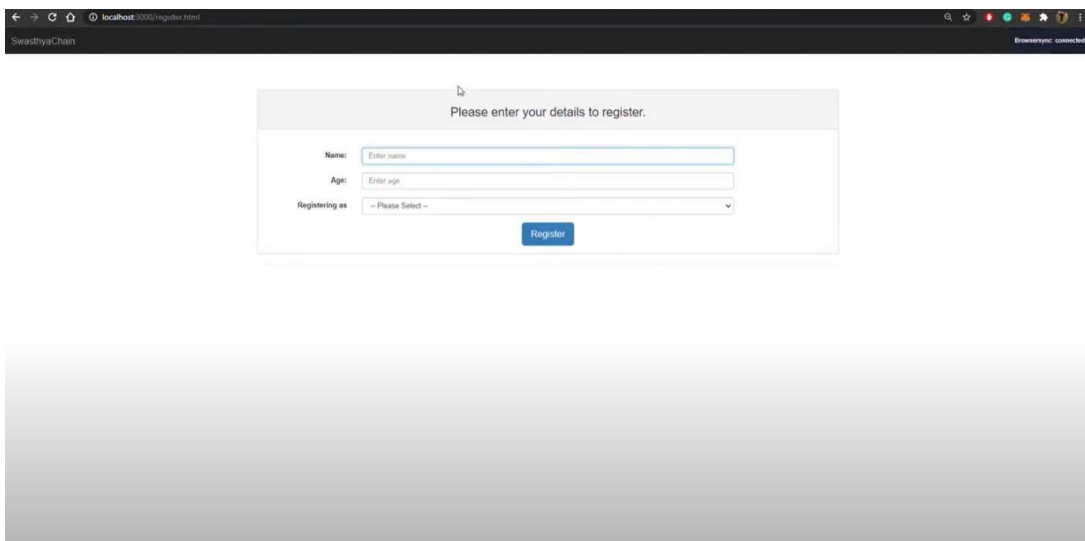
A screenshot of a web browser displaying a registration form. The browser's address bar shows 'localhost:3000/register.html' and the page title is 'SwasthyaChan'. The form itself is centered and has a light gray background. At the top of the form, it says 'Please enter your details to register.' Below this, there are three input fields: 'Name:' with a text box containing 'Enter name', 'Age:' with a text box containing 'Enter age', and 'Registering as:' with a dropdown menu showing '-- Please Select --'. A blue 'Register' button is positioned at the bottom right of the form.

Figure 13: Representation of document verification

It has the following possible effects:

1. Enhanced authentication: Soulbound tokens offer a safe, unchangeable record of a document's validity, which can help lower the possibility of fraud and counterfeiting.

Figure 14 shows enhanced authentication and involves authentication factors(Knowledge factor, possession factor, biometric factor), authentication request where the system sends a request to the user to provide the additional authentication factors based on the chosen methods.

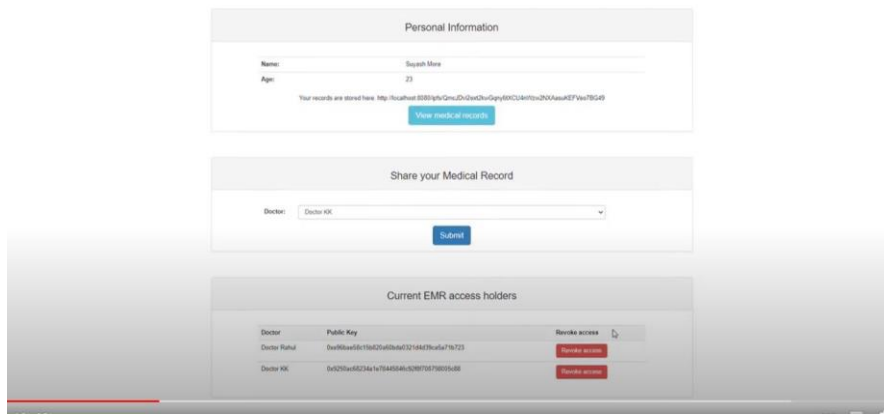


Figure 14: Representation of enhanced authentication

2. Enhanced efficiency: Hospitals can expedite their document verification procedures by employing soulbound tokens, as the blockchain facilitates the rapid and simple authentication of a document's legitimacy.

Figure 15 shows the enhanced efficiency of a system where process optimization, automation, resource allocation, performance monitoring, training and development, and collaboration and communication.

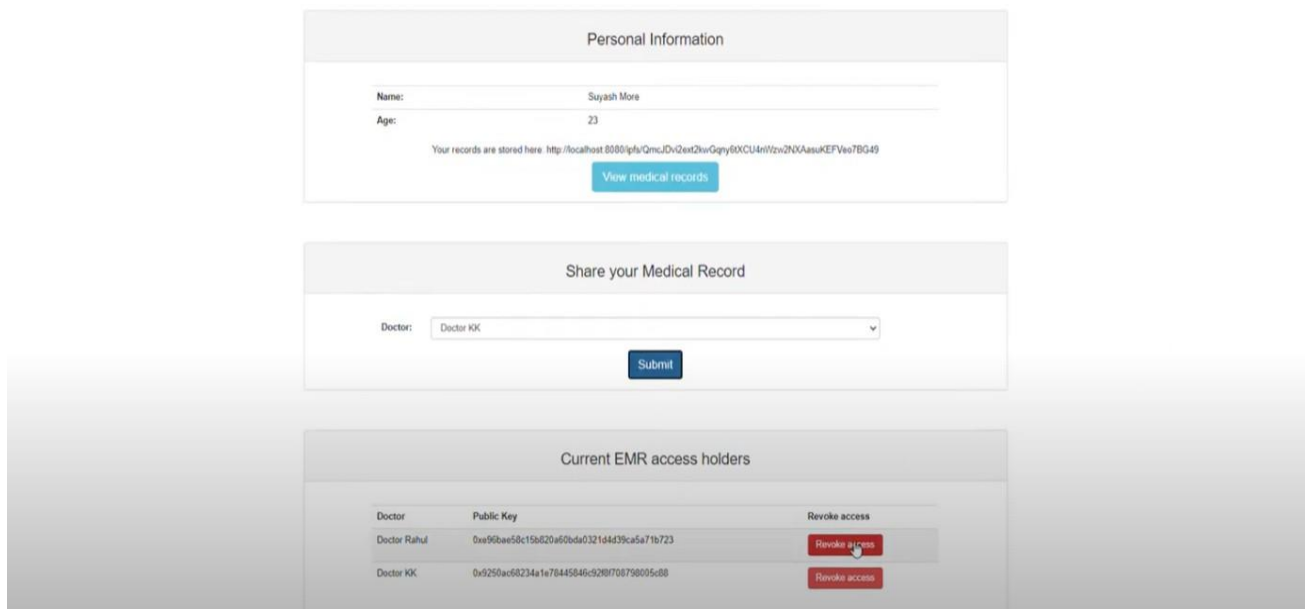


Figure 15: Representation of enhanced efficiency

3. Greater transparency: Soulbound tokens can boost trust in the document verification process by enabling everyone with blockchain access to confirm a document's legitimacy.

Figure 16 shows information accessibility, open communication, data sharing, decision-making process, accountability, compliance, and regulations.

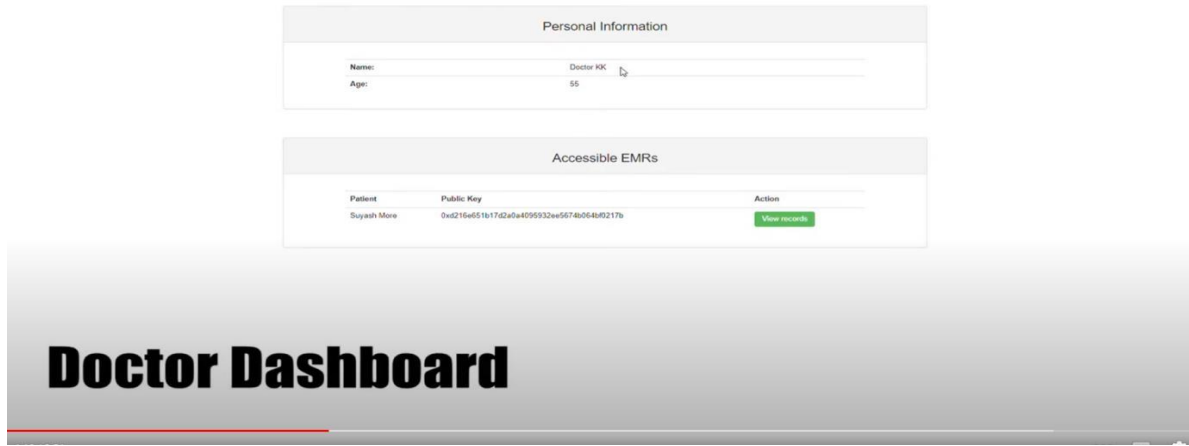


Figure 16: Representation of greater transparency

4. Improved interoperability: Soulbound tokens can be used to establish a medical record verification standard that works with many systems and organizations, making it easier to share and use digital data.; Figure 17 shows improved interoperability in a system where data exchange, system integration, cross-platform compatibility, APIs and Interfaces, Data mapping and transformation, and Semantic Interoperability

The image shows a web interface for medical records. The top section is titled "Personal Information" and contains a form with the following fields: "Name: Suyash More" and "Age: 23". Below these fields, there is a URL: "Your records are stored here: http://localhost:8080/pfs/QmccaquUDABJQSP67pyNqjux1ZvkSacU5ECSqPsaF6T4" and a blue button labeled "Hide Medical Records". Below this is a text box containing the following information: "Name: Suyash More", "Pub1k key: 0xd216e6511702a8a4095932ee5674b864c4f8217b", "Diagnosed By: Doctor XX", "Diagnosis Time: 13/05/2021 17:20 PM", "Diagnosis: Covid-19", "Comments: Ct Score:19", and "Home Quarantine". The bottom section is titled "Share your Medical Record" and contains a dropdown menu for "Doctor" with the text "-- Please Select --" and a blue button labeled "Submit". Below this is a section titled "Current EMR access holders".

Figure 17: Representation of improved interoperability

4.1 Context of Simulation

Figure 18 shows the number of hashes needed to establish a selective disclosure credential. Our simple public cryptography strategy is compared to the merkle tree selective disclosure method in this paper. The number of hashes needed to confirm selective disclosure credentials is shown in Figure 19. Our method has constant time, unlike the merkle tree approach, which takes $\text{Log}(N)$.

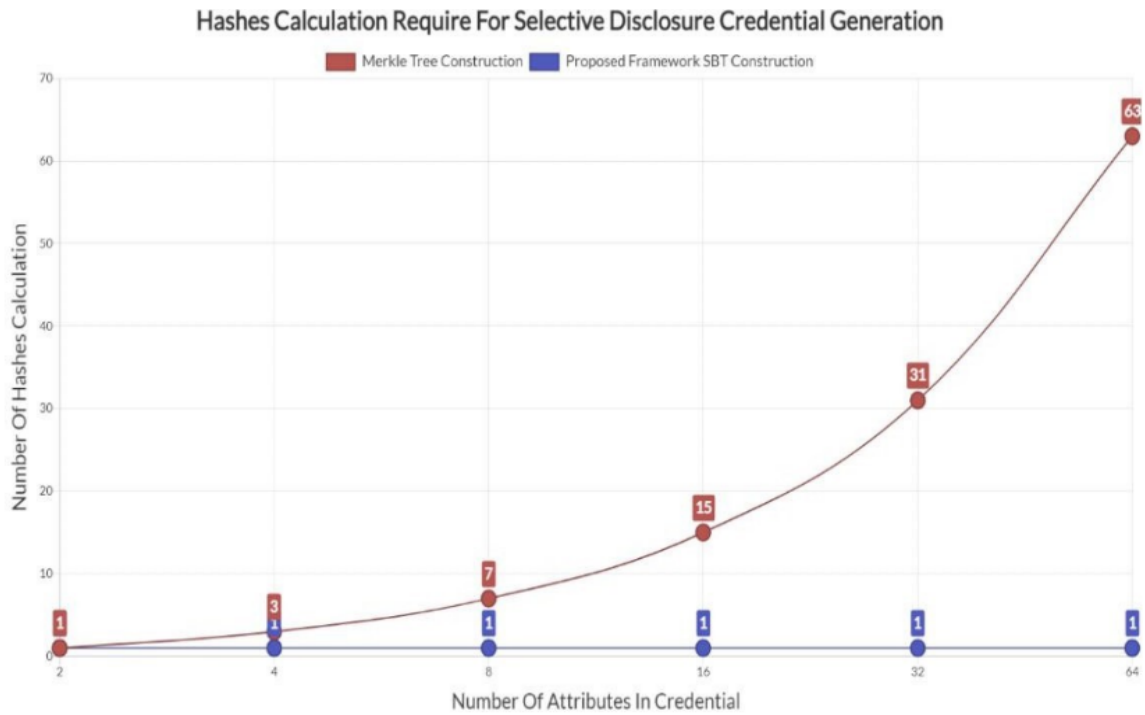


Figure 18: Comparison between Merkle tree and selective disclosure credential generation

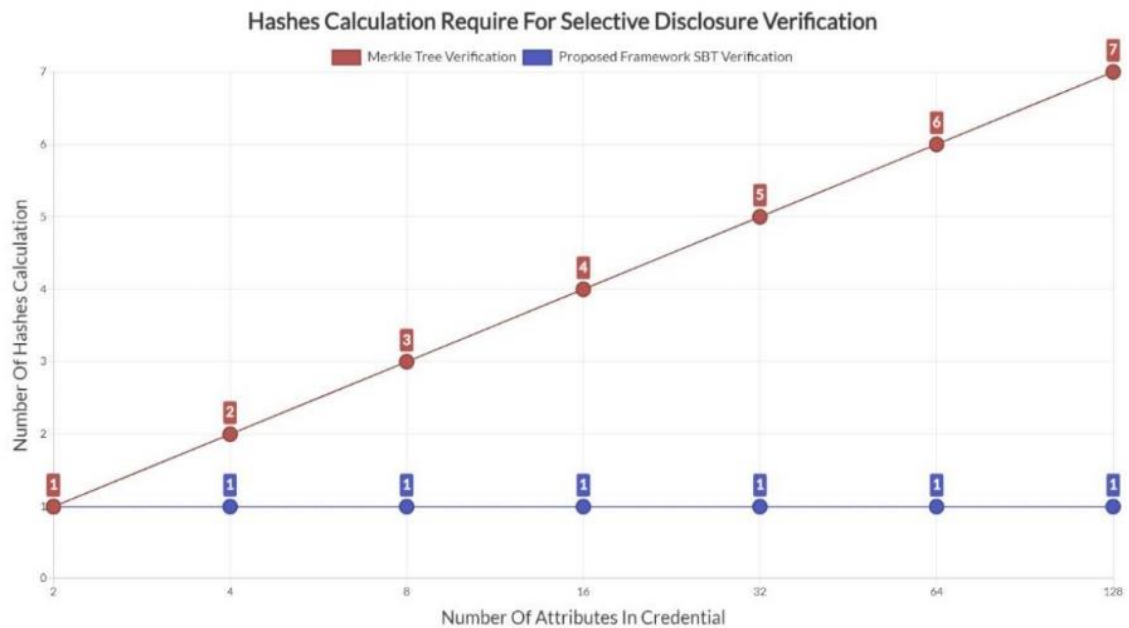


Figure 19: Comparison between Merkle tree and selective disclosure credential verification

5. Conclusion

Our suggested architecture for a blockchain-based credential verification system can offer a safe, dependable means of confirming the legitimacy of credentials and thwarting fraud. A decentralized, tamper-proof credential database that is transparently and securely accessible to authorized parties can be established by a credential verification system. Furthermore, real-time credential verification via a blockchain-based credential verification system can assist people and businesses make better decisions and lower their risk of credential fraud. In general, the implementation of a blockchain-based credential verification system can yield noteworthy advantages concerning security, dependability, and productivity. This framework has a wide range

of applications in which it can be used to address practical issues. This system can resolve time-consuming, recurring KYC (know your customer) verification issues for a variety of enterprises. The issue is that at the initial registration phase, KYC must be completed for every firm. Giving the person a soulbound token once they've finished the KYC is one way to go about it. After that, organizations can use this SBT of completeness to leverage blockchain identity verification. Popular cryptocurrency exchange Binance offers BAB (Binance accountbound token) to users who successfully complete the platform's KYC procedure as an example of one potential implementation. The other use case is using the blockchain to store personal credentials or papers (such as a driver's license or passport). The framework's ability to protect data privacy allows it to conceal documents from public view. Blockchain technology will eliminate documents that are not authorized from the server and prevent credential forgery. This concept can be applied to hiring procedures at businesses. A candidate's prior work history is sometimes required for job vacancies in order to verify their suitability for the role. Every task or accomplishment that an employee completes while employed by the organization is eligible for an SBT from the employer. Anyone, from anywhere in the globe, can verify these SBTs. Blockchain technology will improve efficiency, decrease friction in the current system, and lessen false experience claims.

Declarations

Author Contributions: All authors contributed equally to the conceptualization, formal analysis, investigation, methodology, and writing and editing of the original draft. All authors have read and agreed to the published version of the manuscript.

Acknowledgments: This research was financially supported by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2024R237), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University (KKU) for funding this research through the Research Group Program Under the Grant Number: (R.G.P.2/451/44).

Funding: This research was financially supported by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2024R237), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University (KKU) for funding this research through the Research Group Program Under the Grant Number: (R.G.P.2/451/44).

Availability of data and materials: The datasets used during the current study are available from the corresponding author on reasonable request.

Ethics approval and consent to participate: Not applicable.

Consent for publication: Not applicable.

Competing interests: The authors declare no competing interests.

References

- [1]. Villarreal, E. R. D., García-Alonso, J., Moguel, E., & Alegría, J. A. H. (2023). Blockchain for healthcare management systems: A survey on interoperability and security. *IEEE Access*, 11, 5629-5652.

- [2]. Singh, P., & Verma, S. (2019). Analysis on Different Strategies Used in Blockchain Technology. *Journal of Computational and Theoretical Nanoscience*, 16(10), 4350-4355.
- [3]. Araujo-Inastrilla, C. R., & Vitón-Castillo, A. A. (2023). Blockchain in health sciences: Research trends in Scopus. *Iberoamerican Journal of Science Measurement and Communication*, 3(2).
- [4]. Lakhan, A., Mohammed, M. A., Nedoma, J., Martinek, R., Tiwari, P., & Kumar, N. (2023). DRLBTS: deep reinforcement learning-aware blockchain-based healthcare system. *Scientific Reports*, 13(1), 4124.
- [5]. Ahmad, S., Arya, S. K., Gupta, S., Singh, P., & Dwivedi, S. K. (2023, May). Study of Cryptographic Techniques Adopted in Blockchain. In *2023 4th International Conference on Intelligent Engineering and Management (ICIEM)* (pp. 1-6). IEEE.
- [6]. Kaushik, K., & Kumar, A. (2023). Demystifying quantum blockchain for healthcare. *Security and Privacy*, 6(3), e284.
- [7]. Sun, M., Chai, Q., & Ng, C. T. (2023). Managing the quality-speed tradeoff in blockchain-supported healthcare diagnostic services. *Omega*, 102911.
- [8]. Tareen, F. N., Alvi, A. N., Malik, A. A., Javed, M. A., Khan, M. B., Saudagar, A. K. J., ... & Abul Hasanat, M. H. (2023). Efficient Load Balancing for Blockchain-Based Healthcare System in Smart Cities. *Applied Sciences*, 13(4), 2411.
- [9]. Bennacer, S. A., Sabiri, K., Aaroud, A., Akodadi, K., & Cherradi, B. (2023). A comprehensive survey on blockchain-based healthcare industry: Applications and challenges. *Indones. J. Electr. Eng. Comput. Sci*, 30, 1558-1571.
- [10]. Singh, P., Singh, A.P. and Gupta, A. 2021. Design Strategies for Mobile Ad-hoc Network to Prevent from Attack. *Proceedings of the 3rd International Conference on Advanced Computing and Software Engineering*. SCITEPRESS - Science and Technology Publications.
- [11]. Aloini, D., Benevento, E., Stefanini, A., & Zerbino, P. (2023). Transforming healthcare ecosystems through blockchain: Opportunities and capabilities for business process innovation. *Technovation*, 119, 102557.
- [12]. Hajian, A., Prybutok, V. R., & Chang, H. C. (2023). An empirical study for blockchain-based information sharing systems in electronic health records: A mediation perspective. *Computers in Human Behavior*, 138, 107471.
- [13]. Hegde, P., & Maddikunta, P. K. R. (2023). Secure PBFT Consensus-Based Lightweight Blockchain for Healthcare Application. *Applied Sciences*, 13(6), 3757.
- [14]. Wenhua, Z., Qamar, F., Abdali, T. A. N., Hassan, R., Jafri, S. T. A., & Nguyen, Q. N. (2023). Blockchain technology: security issues, healthcare applications, challenges and future trends. *Electronics*, 12(3), 546.
- [15]. Singh, P., Sinha, P., & Raghav, A. (2023). A Blockchain IoT Hybrid Framework for Security and Privacy in a Healthcare Database Network. In *Dynamics of Swarm Intelligence Health Analysis for the Next Generation* (pp. 210-225). IGI Global.

- [16]. Sharma, P., Namasudra, S., Crespo, R. G., Parra-Fuente, J., & Trivedi, M. C. (2023). EHDHE: Enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain. *Information Sciences*, 629, 703-718.
- [17]. Ali, A., Al-Rimy, B. A. S., Alsubaei, F. S., Almazroi, A. A., & Almazroi, A. A. (2023). HealthLock: Blockchain-Based Privacy Preservation Using Homomorphic Encryption in Internet of Things Healthcare Applications. *Sensors*, 23(15), 6762.
- [18]. Badri, S., Ullah Jan, S., Alhazzawi, D., Aldhaheri, S., & Pitropakis, N. (2023). BIoMT: A Blockchain-Enabled Healthcare Architecture for Information Security in the Internet of Medical Things.
- [19]. Kiania, K., Jameii, S. M., & Rahmani, A. M. (2023). Blockchain-based privacy and security preserving in electronic health: a systematic review. *Multimedia Tools and Applications*, 1-27.
- [20]. Miriam, H., Doreen, D., Dahiya, D., & Rene Robin, C. R. (2023). Secured Cyber Security Algorithm for Healthcare System Using Blockchain Technology. *Intelligent Automation & Soft Computing*, 35(2).
- [21]. Sinha, P., Singh, R., Roy, R., & Singh, P. (2022, March). Education and Analysis of Autistic Patients Using Machine Learning. In *2022 International Conference on Emerging Smart Computing and Informatics (ESCI)* (pp. 1-6). IEEE.
- [22]. Singh, P., Sinha, P., & Raghav, A. (2023). A Blockchain IoT Hybrid Framework for Security and Privacy in a Healthcare Database Network. In *Dynamics of Swarm Intelligence Health Analysis for the Next Generation* (pp. 210-225). IGI Global.
- [23]. Pathak, R., Soni, B., & Muppalaneni, N. B. (2023, February). Role of Blockchain in Health Care: A Comprehensive Study. In *Proceedings of 3rd International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications: ICMISC 2022* (pp. 137-154). Singapore: Springer Nature Singapore.
- [24]. Elgamal, E., Medhat, W., Abd Elfatah, M., & Abdelbaki, N. (2023, January). Blockchain in Healthcare for Achieving Patients' Privacy. In *2023 20th Learning and Technology Conference (L&T)* (pp. 59-64). IEEE.
- [25]. David, S., Duraipandian, K., Chandrasekaran, D., Pandey, D., Sindhvani, N., & Pandey, B. K. (2023). Impact of blockchain in healthcare system. In *Unleashing the Potentials of Blockchain Technology for Healthcare Industries* (pp. 37-57). Academic Press.
- [26]. Vishwakarma, A., Dangayach, G. S., Meena, M. L., Gupta, S., & Luthra, S. (2023). Adoption of blockchain technology enabled healthcare sustainable supply chain to improve healthcare supply chain performance. *Management of Environmental Quality: An International Journal*, 34(4), 1111-1128.
- [27]. Karmakar, A., Ghosh, P., Banerjee, P. S., & De, D. (2023). ChainSure: Agent-free insurance system using blockchain for healthcare 4.0. *Intelligent Systems with Applications*, 17, 200177.
- [28]. Karmakar, A., Ghosh, P., Banerjee, P. S., & De, D. (2023). ChainSure: Agent free insurance system using blockchain for healthcare 4.0. *Intelligent Systems with Applications*, 17, 200177.

- [29]. Singh, P., & Sagar, S. (2023). Transaction Delay Of Data Transmission Between Sensor And Blockchain Technology For The Healthcare Domain Using Consensus Mechanism. *Russian Law Journal*, 11(13s).
- [30]. Singh, P., & Sagar, S. (2024). Healthcare monitoring system with blockchain technology encompassing energy harvesting and delays in a Wideband Network. *Journal of Integrated Science and Technology*, 12(4), 794-794.
- [31]. Bhadoria, R., Singh, P., & Ahmad, S. (2023, June). A Comprehensive Study of Blockchain Technology Trends and Analysis in the Healthcare Industry 4.0. In *International Conference on Recent Developments in Cyber Security* (pp. 567-581). Singapore: Springer Nature Singapore.