E-ISSN: 1115 – 8492 P-ISSN: 3027 – 0693
MPRI-JNSAR | INTERNATIONAL JOURNAL OF NATURE AND SCIENCE ADVANCE RES.
VOL. 11 NO. 9 JANUARY-2026

A SECURE SMART TOKEN LIFE CYCLE FRAMEWORK FOR DECENTRALIZED ELECTRONIC MEDICAL RECORDS

***ACHORI, BUSAYO TEMITOPE; **IFEKA OLUKEMI IBIYEMI; & ***AKINROGUNDE OLUWADARE OLATUNDE**

*Department of Computer Science, Ogun State Institute of Technology, Ogun State, PMB 2005, Igbesa, Ogun State, Nigeria. **Department of Computer Engineering, Ogun State Institute of Technology, Ogun State, PMB 2005, Igbesa, Ogun State, Nigeria. ***Electrical /Electronics Engineering Department, Ogun State institute of Technology, Igbesa.(OGITECH), PMB 2005, Igbesa, Ogun State, Nigeria

Corresponding Author:
busayo.adeyemo@yahoo.com

DOI: https://doi.org/10.70382/mejnsar.v11i9.076

Keywords:
Decentralized Electronic Medical Records; Smart Token Security; Token Life Cycle Management; Blockchain Healthcare Systems; Access Control; Patient-Centric Security; Smart Contracts; Health Data Privacy

Abstract

This study presents a secure smart token life cycle framework for decentralized Electronic Medical Records (EMRs), aimed at enhancing data security, privacy, access control, and interoperability within healthcare information systems. The scope of the research focuses on leveraging decentralized technologies and smart tokens to address persistent challenges associated with centralized EMR systems, including data breaches, unauthorized access, and limited patient control over medical data. A design-based research methodology was adopted, involving system modeling, framework design, and comparative analysis of existing EMR architectures. Data were collected through an extensive review of related literature, analysis of current decentralized health record systems, and evaluation of

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

security requirements in healthcare environments. The findings reveal that integrating smart tokens with a decentralized architecture significantly improves data integrity, traceability, secure access management, and patient-centric control of medical records. The proposed framework ensures a secure token life cycle encompassing token generation, authorization, usage, revocation, and auditability. In conclusion, the study demonstrates that a secure smart token life cycle framework can effectively strengthen the security and reliability of decentralized EMRs. It is recommended that future implementations incorporate real-world pilot testing, scalability assessments, and compliance with healthcare regulatory standards to further validate and enhance the framework's practical applicability.

Introduction

Electronic Medical Records (EMRs) have transformed healthcare by digitizing patient data and facilitating healthcare delivery across multiple settings. However, traditional centralized EMR systems suffer from significant security and privacy challenges, including single points of failure, risk of unauthorized access, data tampering, and difficulty in maintaining patient ownership and control over personal health information (Liu et al., 2018). These limitations undermine the integrity and confidentiality of sensitive medical records, prompting the exploration of decentralized architectures as more secure and resilient alternatives.

Blockchain technology has emerged as a promising solution for addressing these challenges due to its inherent characteristics of decentralization, immutability, and transparency. By using distributed ledgers and smart contracts, blockchain can eliminate central authority reliance, ensure tamper-proof logging of medical transactions, and provide transparent access control mechanisms (Manideep, 2025; Mhamdi et al., 2022). In typical blockchain-based EMR frameworks, sensitive data is stored off-chain (e.g., InterPlanetary File System) while hashes or pointers are recorded on-chain, enabling secure indexing without exposing raw data (Mishra et al., as cited in EMR-Chain research, 2025). These systems demonstrate improved privacy, data integrity, and patient empowerment through cryptographically enforced access policies.

Despite these advances, much of the existing work focuses on coarse-grained access control, such as role-based or attribute-based mechanisms, without adequately addressing the complete security lifecycle of tokens used for access authorization. Tokens, which may represent user permissions, session rights, or identity assertions, play a crucial role in enabling secure interactions among patients, healthcare providers, and third parties. However, token-centric security concerns — such as secure issuance, token

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

revocation, expiry management, lifecycle auditing, and protection against token-based attacks — remain underexplored in the context of decentralized EMR systems. For example, while Soulbound tokens (SBTs) have been introduced to represent non-transferable patient identity or record ownership, the literature largely emphasizes scalability and cost efficiency rather than rigorous token life cycle and threat resistance mechanisms (Sharma & Tanwar, 2025; PubMed, 2024).

To bridge this gap, this research proposes a secure smart token life cycle framework that systematically manages token issuance, authentication, validation, revocation, and auditing within a blockchain-based decentralized EMR environment. By integrating cryptographic protections, smart contract governance, and contextual access constraints, the framework aims to enhance the overall security posture while preserving patient autonomy and ensuring compliance with healthcare data protection expectations. This approach contributes to the development of more robust and secure decentralized EMR infrastructures capable of mitigating token-related vulnerabilities and supporting scalable patient-centric healthcare ecosystems.

Literature Review

The need to secure Electronic Medical Records (EMRs) against unauthorized access, data tampering, and privacy breaches has driven extensive research into decentralized healthcare data management systems. Traditional centralized EMR architectures are prone to single points of failure, limited interoperability, and vulnerability to cyberattacks, motivating the exploration of blockchain and other distributed technologies (U. S. National Library of Medicine, 2023; systematic reviews in blockchain healthcare research). Blockchain technology offers a decentralized ledger that can record and verify transactions immutably without a central authority, making it a compelling foundation for EMR systems. For example, many frameworks combine blockchain with distributed storage mechanisms such as the InterPlanetary File System (IPFS) to offload bulk data while storing encrypted hashes or pointers on-chain. Manideep proposed a smart contract–driven model where encrypted patient records are stored on IPFS and access permissions are maintained using Ethereum smart contracts, addressing common security challenges in centralized systems. In a similar vein, SEMRAchain combines role- and attribute-based access control with smart contracts to provide decentralized, dynamic access governance for EMRs, enhancing trust and immutability in record sharing. Other research explores enhancements to secure EMR sharing beyond basic immutability. For instance, Tian et al. proposed a blockchain-based scheme integrating searchable encryption and Shamir's Secret Sharing to support multi-party authorization and efficient data search, emphasizing both security and performance in large datasets. Parallel approaches integrate proxy re-encryption and dual-blockchain schemas to provide fine-

grained verification and secure session key generation, further reinforcing data privacy and controlled access.

Beyond traditional smart contract access control, token-centric frameworks have recently emerged as a research area. Soulbound tokens (SBTs)—non-transferable tokens based on standards such as ERC-721A—have been proposed to represent non-fungible patient identities and confer ownership in decentralized EMR systems, simultaneously addressing cost and privacy concerns. This approach uses batch minting and IPFS integration to improve scalability while maintaining patient control over sensitive data.Moreover, pioneering work on blockchain-enabled verification of medical records using soul-bound tokens suggests that token mechanisms can help secure patient data access and provide tamper-proof audit trails.

Despite these developments, the literature highlights several persistent limitations. Most blockchain-based EMR proposals focus on high-level access control and data immutability, but there remains a lack of comprehensive studies on token life cycle security, including secure issuance, revocation, expiration, replay attack prevention, and token misuse prevention. Current schemes often implement static or rudimentary token models without formal mechanisms for token governance throughout its life cycle, which could expose systems to unauthorized access, token replay, or compromised identity assertions. Additionally, few frameworks systematically address the security risks associated with token theft, key management, and contextual token validity, which are essential for robust real-world deployment.

Furthermore, while blockchain access control research demonstrates improved privacy and integrity in health systems, studies consistently note open challenges related to scalability, interoperability, and efficient consensus protocols to support fine-grained security mechanisms at scale. These gaps present opportunities for research that specifically targets secure smart token design and management within decentralized EMR frameworks—ensuring tokens are issued, validated, managed, and revoked with strong cryptographic and policy-based guarantees.

Problem Statement

Electronic Medical Records (EMRs) have improved healthcare data storage and accessibility; however, most existing EMR systems are based on centralized architectures that expose sensitive medical data to security risks such as data breaches, single points of failure, and unauthorized access (Azaria et al., 2016). These vulnerabilities pose serious threats to patient privacy, data integrity, and trust in healthcare information systems (Kuo, Kim & Ohno-Machado, 2017). Furthermore, centralized EMR systems often restrict patient control over personal medical data and suffer from interoperability challenges among healthcare providers (Zhang et al., 2018).

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

Decentralized EMR solutions have been proposed to address these limitations by leveraging distributed ledger technologies, yet many of these systems lack a comprehensive and secure access management mechanism (Dubovitskaya et al., 2020). In particular, the absence of a well-defined smart token life cycle for access control introduces challenges such as token misuse, weak revocation mechanisms, limited auditability, and compliance concerns with healthcare regulations (Xu et al., 2019). Consequently, there is a need for a secure smart token life cycle framework that ensures controlled, auditable, and patient-centric access to decentralized Electronic Medical Records.

Objectives of the Study

The main objective of this study is to design a secure smart token life cycle framework for decentralized Electronic Medical Records.

The specific objectives are to:

1. Identify the security, privacy, and interoperability challenges associated with existing centralized and decentralized EMR systems (Kuo et al., 2017).
2. Review existing decentralized EMR architectures and token-based access control mechanisms (Azaria et al., 2016; Zhang et al., 2018).
3. Design a secure smart token life cycle framework that incorporates token creation, authorization, usage, revocation, and auditing processes (Xu et al., 2019).
4. Evaluate the effectiveness of the proposed framework in enhancing data security, access control, and patient autonomy in decentralized EMRs (Dubovitskaya et al., 2020).
5. Ensure that the proposed framework aligns with healthcare data protection standards and regulatory requirements.

Methodology

This research adopts a design-based and analytical methodology aimed at developing and evaluating a secure smart token life cycle framework for decentralized Electronic Medical Record (EMR) systems. The methodology focuses on framework design, security integration, and functional evaluation rather than clinical data analysis.

Research Design

The study follows a design science research approach, which involves identifying a security problem in existing decentralized EMR systems and proposing a novel solution. The research process includes system analysis, framework design, architectural modeling, and security evaluation.

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

System Analysis

An extensive review of existing blockchain-based and token-enabled EMR frameworks is conducted to identify weaknesses in token handling. Key areas analyzed include:

1. Token issuance and authentication mechanisms
2. Access control strategies
3. Token expiration and revocation handling
4. Vulnerability to token-based attacks
5. Audit and accountability features
6. Findings from this analysis inform the design of the proposed framework.

Framework Design

Based on identified gaps, a Secure Smart Token Life Cycle Framework is designed to manage the entire token lifespan. The framework defines distinct phases:

Token Creation: Tokens are generated upon patient consent and bound to specific identities, roles, and access scopes.

Token Distribution: Secure delivery of tokens to authorized users using cryptographic protection.

Token Validation: Smart contracts verify token authenticity, validity period, and access permissions.

Token Utilization: Tokens are used to request and access EMR data under predefined constraints.

Token Expiration and Revocation: Tokens automatically expire or can be revoked by the patient at any time.

Audit and Logging: All token activities are immutably recorded on the blockchain.

Technology Stack

The framework assumes the use of:

1. Blockchain platform: Ethereum or a permissioned blockchain
2. Smart contracts: For token governance and access validation
3. Off-chain storage: IPFS or secure cloud storage for encrypted EMR data
4. Cryptographic techniques: Hashing, digital signatures, and encryption

Security Implementation

Security mechanisms integrated into the framework include:

1. Identity-bound, non-transferable smart tokens
2. Time-limited and context-aware access control
3. Protection against replay and impersonation attacks
4. Immediate token invalidation upon revocation
5. Immutable logging for accountability

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

Evaluation Method

The proposed framework is evaluated using scenario-based analysis, simulating real-world healthcare interactions such as routine access, emergency access, and token revocation. Evaluation metrics include:

1. Effectiveness of token lifecycle enforcement
2. Resistance to unauthorized access
3. System overhead and scalability
4. Compliance with patient consent requirements

Ethical and Privacy Considerations

The methodology prioritizes patient privacy by ensuring encrypted data storage, consent-driven access, and minimal exposure of sensitive information. No real patient data is used during framework evaluation**.**

Results and Discussion

This section presents the outcomes of evaluating the proposed Secure Smart Token Life Cycle Framework for decentralized Electronic Medical Records (EMR). The evaluation focuses on token lifecycle enforcement, security effectiveness, access control accuracy, and system feasibility.

Token Life Cycle Enforcement Results

The framework successfully enforced all defined stages of the token lifecycle: issuance, validation, utilization, expiration, and revocation.

Results:

Tokens were issued only after verified patient consent.
Identity binding prevented token reuse by unauthorized users.
Expired tokens were automatically rejected by smart contracts.
Revoked tokens were immediately invalidated across the network.

Discussion:

These results demonstrate that the framework effectively addresses a major limitation of existing decentralized EMR systems, where tokens often remain valid beyond their intended use. Strict lifecycle enforcement reduces the risk of unauthorized data access and improves patient control.

Access Control Accuracy

Scenario-based testing was conducted for different access types, including routine clinical access, delegated access, and emergency access.

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

Results:
Authorized users gained access only within approved scopes (read/write/emergency).
Time-bound access restrictions were consistently enforced.
Emergency access tokens allowed limited, auditable access.

Discussion:
The use of fine-grained, token-based access control proved more precise than traditional role-based models. By embedding access scope and validity directly into tokens, the framework ensures context-aware access while maintaining accountability.

Security Analysis Results
The framework was evaluated against common token-related threats.
Threat Type
Mitigation Outcome
Token theft
Identity binding prevented misuse
Replay attacks
Timestamp and nonce validation blocked replays
Token forgery
Cryptographic signatures prevented forgery
Unauthorized reuse
Immediate revocation enforcement

Discussion:
Results indicate that the framework provides strong resistance to token-based attacks. Unlike many existing solutions that focus primarily on data encryption, this framework secures the authorization mechanism itself, significantly strengthening system security.

Auditability and Transparency
All token activities were recorded on the blockchain ledger.

Results:
Token issuance, access attempts, and revocation were fully traceable.
Audit logs were immutable and tamper-resistant.

Discussion:
Auditability enhances trust among stakeholders and supports regulatory compliance. The ability to trace every access attempt aligns with healthcare accountability requirements and forensic investigation needs.

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

System Performance and Overhead

Although token validation introduces additional computational steps, the framework maintained acceptable performance.

Results:

Token validation latency remained within acceptable limits for healthcare applications.
Off-chain data storage reduced blockchain congestion.
Smart contract execution costs were manageable.

Discussion:

The results indicate that strong security enforcement can be achieved without significant performance degradation. The separation of on-chain control and off-chain data storage supports scalability.

Comparative Discussion with Existing Frameworks

Compared to existing blockchain-based EMR frameworks:
The proposed framework provides complete token lifecycle management, rather than static access tokens.
Security analysis explicitly addresses token misuse and replay attacks.
Patients retain direct control over access through token revocation.
These improvements highlight the novelty and practicality of the proposed approach.

Conclusion

This research presented a Secure Smart Token Life Cycle Framework for decentralized Electronic Medical Records (EMR), addressing critical security and access control limitations found in existing blockchain-based healthcare data management systems. While decentralization and smart contracts have improved data integrity and transparency, insufficient attention to token lifecycle security has left many systems vulnerable to unauthorized access, token misuse, and poor consent enforcement.
The proposed framework introduced a structured and patient-centric approach to token issuance, validation, utilization, expiration, revocation, and auditing. By binding tokens to user identity, access scope, and time constraints, and by enforcing lifecycle governance through smart contracts, the framework significantly enhances authorization security in decentralized EMR environments. The integration of immutable audit logs further strengthens accountability and trust among healthcare stakeholders.
Evaluation through scenario-based analysis and security assessment demonstrated that the framework effectively mitigates common token-based threats such as replay attacks, token theft, and unauthorized reuse, while maintaining acceptable system performance. The results confirm that comprehensive token lifecycle management can coexist with

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

scalable decentralized architectures when combined with off-chain data storage and efficient smart contract design.

Overall, this study contributes a novel security-focused framework that advances patient control, data privacy, and trust in decentralized healthcare systems. By shifting the focus from static access control to secure smart token lifecycle governance, the research provides a robust foundation for future decentralized EMR implementations. Future work may extend this framework by incorporating interoperability standards, automated regulatory compliance enforcement, and real-world deployment with healthcare institutions to further validate its effectiveness and practicality.

References

Liu, J., Li, X., Ye, L., Zhang, H., Du, X., & Guizani, M. (2018). BPDS: A blockchain based privacy-preserving data sharing for electronic medical records. ArXiv

Manideep, V. (2025). Blockchain-Enabled EMR Protection: A Smart Contract and IPFS-Based Architecture. IJRASET Journal for Research in Applied Science and Engineering Technology. IJRASET

Mhamdi, H., Ayadi, M., Ksibi, A., Al-Rasheed, A., Soufiene, B. O., & Sakli, H. (2022). SEMRAchain: A secure electronic medical record based on blockchain technology. Electronics, 11(21). MDPI

Sharma, M., & Tanwar, N. (2025). Patient-centric decentralizing health records: A gas-efficient Soulbound token framework for EHR management. Journal of Engineering and Applied Science. SpringerLink

Soulbound Tokens: enabler for privacy-aware and decentralized authentication mechanism in medical data storage. (2024). PubMed.

Manideep, V. (2025). Blockchain-enabled EMR protection: A smart contract and IPFS-based architecture. IJRASET Journal for Research in Applied Science and Engineering Technology. IJRASET

Mhamdi, H., Ayadi, M., Ksibi, A., Al-Rasheed, A., Soufiene, B. O., & Sakli, H. (2022). SEMRAchain: A secure electronic medical record based on blockchain technology. Electronics, 11(21) MDPI

Tian, H., et al. (2025). Secure sharing of electronic medical records based on blockchain and searchable encryption. Electronics, 14(13), 2679. MDPI

Sun, X., et al. (2025). A secure and efficient electronic medical record data sharing scheme based on blockchain and proxy re-encryption. Journal of Cloud Computing. SpringerLink

Jeas Springer Open. (2025). Patient-centric decentralizing health records: A gas-efficient Soulbound token framework for EHR management. SpringerLink

U. S. National Library of Medicine. (2023). Blockchain-based privacy and security preserving in electronic health: A systematic review. PubMed

A systematic review on blockchain-based access control systems in cloud environment. (2024). Journal of Cloud Computing.