ISSN 2277-2685
IJESR/April. 2026/ Vol-16/Issue-2s1/219-225
Mohd Abdul Muqthadir *et. al.*, / International Journal of Engineering & Science Research
Full Length Article

Fort2bck: Hybrid Cryptographic Validation For Robust Healthcare Data Protection

Mohd Abdul Muqthadir[1], Abdul Samad[2], Mrs. Heena Yasmin[3]
[1,2]B.E.Students; Department Of Computer Science Engineering ISL Engineering College Hyderabad India
Assistant Professor; Department Of Computer Science Engineering ISL Engineering College Hyderabad India
Mail Id; *abdulmuqthadir0786@gmail.com* ,abdulsamad94414@gmail.com
Accepted 27-04-2026

Abstract
Fort2BCK is a robust security framework designed to address major vulnerabilities in healthcare blockchain systems, including data tampering, unauthorized access, and limitations in consensus protocols. The framework introduces a dual-layer verification mechanism that strengthens existing consensus algorithms using advanced cryptographic techniques such as RSA, ECDSA, and Zero-Knowledge Proofs (ZKPs). This additional security layer improves authentication, auditability, and resistance against malicious activities within system.

Keywords: *Healthcare Blockchain, Fort2BCK, Cryptographic Validation, RSA, ECDSA, Zero-Knowledge Proofs (ZKP), Data Security, Consensus Protocols, Blockchain Security, Healthcare Data Protection.*

INTRODUCTION

The healthcare industry is rapidly adopting digital technologies such as Electronic Health Records (EHRs), cloud computing, and Internet of Medical Things (IoMT) devices to improve patient care, medical data management, and information sharing. Although these technologies increase efficiency and accessibility, they also introduce major security and privacy challenges, including data breaches, unauthorized access, cyberattacks, and data tampering. Blockchain technology has emerged as a promising solution due to its decentralized, transparent, and tamper-resistant nature; however, existing blockchain systems still face limitations such as scalability issues, consensus protocol vulnerabilities, high computational costs, and attacks like 51% attacks and double-spending. In addition, many blockchain frameworks struggle to meet strict healthcare regulations such as HIPAA and GDPR. To address these issues, this paper proposes Fort2BCK, a Hybrid Cryptographic Validation Framework for Robust Healthcare Data Protection. The framework introduces a dual-layer verification mechanism that combines blockchain consensus protocols with advanced cryptographic techniques including RSA, Elliptic Curve Digital Signature Algorithm (ECDSA), and Zero-Knowledge Proofs (ZKPs) to enhance authentication, data integrity, privacy, and auditability. Unlike traditional blockchain systems, Fort2BCK independently validates each block before it is added to the blockchain, significantly reducing fraudulent transactions and malicious modifications.

LITERATURE REVIEW

A. Cervera García and A. Goussens (2024) proposed a healthcare cybersecurity framework that integrates ICT and blockchain technologies to secure digital healthcare infrastructures. Their work focuses on protecting Electronic Health Records (EHRs) using cryptographic methods such as RSA, ECDSA, and Zero-Knowledge Proofs (ZKPs) while ensuring compliance with HIPAA and GDPR standards.N. Ettaloui, S. Arezki, and T. Gadi (2024) presented a blockchain-based Electronic Health Record (EHR) system integrated with Artificial Intelligence (AI). Their framework improves data privacy, secure data sharing, access control, and regulatory compliance through blockchain technology, smart contracts, and advanced cryptographic techniques.P. Verma, V. Tripathi, and B. Pant (2024) introduced ZeroMedChain, a Layer 2 blockchain security framework for decentralized identity and access management in healthcare. The system uses Zero-Knowledge Proofs (ZKPs), decentralized identity management, and smart contracts to enhance scalability, privacy, and secure healthcare data access

METHODOLOGY

A. Block Chain

The Block chain module serves as the core structural and security backbone of the Fort2BCK project. It manages the distributed ledger system, where all medical transactions—file uploads, report transfers, and approvals—are stored across multiple nodes to prevent a single point of failure. Each block contains

encrypted file data, hash values, timestamps, and digital signatures, linked securely through previous and current hashes. This decentralized approach ensures data immutability, traceability, and fault tolerance.

***B.* Fort2BCK**

The Fort2BCK module represents the heart of the project's security innovation, combining dual-layer verification, cryptographic assurance, and regulatory compliance into a unified framework. It integrates advanced cryptographic techniques such as RSA, ECDSA, and Zero-Knowledge Proofs (ZKPs) to enhance authentication, auditability, and privacy. The module independently verifies each block before inclusion in the chain, ensuring that no fraudulent or tampered data can enter the block chain

***C.* SHA-256**

The SHA-256 module ensures data integrity and tamper detection across all uploaded and transferred medical records. Every file uploaded by a patient is divided into three blocks, and each block is assigned a unique hash value computed using the SHA-256 algorithm. The system also maintains a previous and current hash linkage, forming an immutable sequence that helps verify whether any data has been altered. Even a single-bit modification in the file changes the hash value, alerting the system to potential tampering. This hashing process forms a vital component of the block chain's immutability and trustworthiness, ensuring that healthcare data remains unaltered, verifiable, and transparent throughout its lifecycle.

***D.* RSA**

The RSA module is the foundation of the project's encryption and decryption processes. It employs asymmetric cryptography, where each user is assigned a unique public and private key pair. When patients upload files, the data is encrypted using the RSA public key, ensuring that only authorized doctors or labs possessing the corresponding private key can decrypt and view the original information.

***E.* JSP Dashboard**

Displays the uploaded encrypted data along with file details and timestamps. It also shows the transaction status, verification results, pending registration details, and overall project modules. The dashboard acts as the user interface for monitoring stored data, status, and user details etc….

IMPLEMENTATION

A. Algorithm

The 8-step training and deployment algorithm:

- **Data Collection** – Collect healthcare records and blockchain transaction data from secure sources.
- **Data Preprocessing** – Clean, organize, and encrypt sensitive healthcare information.
- **Key Generation** – Generate RSA and ECDSA cryptographic keys for secure authentication and digital signatures.
- **Blockchain Setup** – Configure blockchain nodes and choose a consensus mechanism such as PoW, PoS, or DPoS.
- **Hybrid Validation Integration** – Integrate RSA, ECDSA, SHA-256, and Zero-Knowledge Proofs (ZKPs) into the blockchain validation process.
- **Model Training and Testing** – Simulate transactions and test the framework against attacks such as data tampering and unauthorized access.
- **Performance Evaluation** – Measure security, transaction accuracy, attack resistance, and computational overhead.
- **Deployment** – Deploy the Fort2BCK framework on a healthcare blockchain network for secure data management and monitoring.

B. Applications

RSA is used for secure encryption and authentication, ECDSA is used for digital signatures and transaction verification, Zero-Knowledge Proofs (ZKPs) are used for privacy-preserving secure validation, and SHA-256 is used for secure hashing and maintaining blockchain data integrity.

TESTING

A. Unit Testing

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program input produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration.

B. Integration Testing

Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by interface defect. The task of the integration test is to check that components or software applications, e.g. components in a software system or – one step up – software applications at the company level – interact without error.

C. Performance Testing

The Performance test ensures that the output be produced within the time limits, and the time taken by the system for compiling, giving response to the users and request being send to the system for to retrieve the results.

RESULTS

A. Comparative Performance:

Algorithm	Function	Security Level	Purpose in Fort2BCK
RSA	Encryption and Authentication	High	Secures healthcare data and user access
ECDSA	Digital Signature Verification	High	Validates blockchain transactions
Zero-Knowledge Proofs (ZKPs)	Privacy-Preserving Validation	Very High	Protects sensitive patient information
SHA-256	Hashing Algorithm	High	Maintains blockchain integrity and prevents tampering
Proof of Work (PoW)	Consensus Mechanism	High	Secures transaction validation
Proof of Stake (PoS)	Consensus Mechanism	Medium-High	Provides energy-efficient validation
Delegated Proof of Stake (DPoS)	Consensus Mechanism	Medium-High	Enables faster and scalable transaction processing

Table I: Comparative Performance of All Evaluated Algorithms

B. Application Output Screenshots

The following figures present the complete HeartGuard AI web application as developed and deployed.

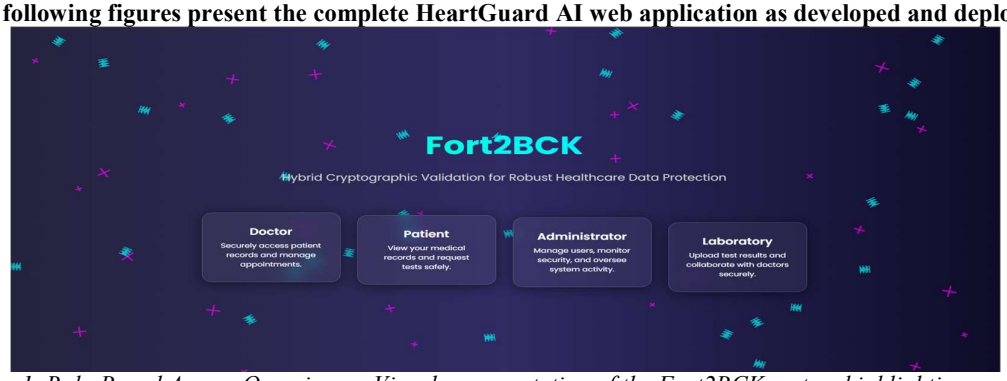

Fig. 1. Role-Based Access Overview — Visual representation of the Fort2BCK system highlighting secure cryptographic validation with distinct functions for doctor, patient, administrator, and laboratory within healthcare data protection.

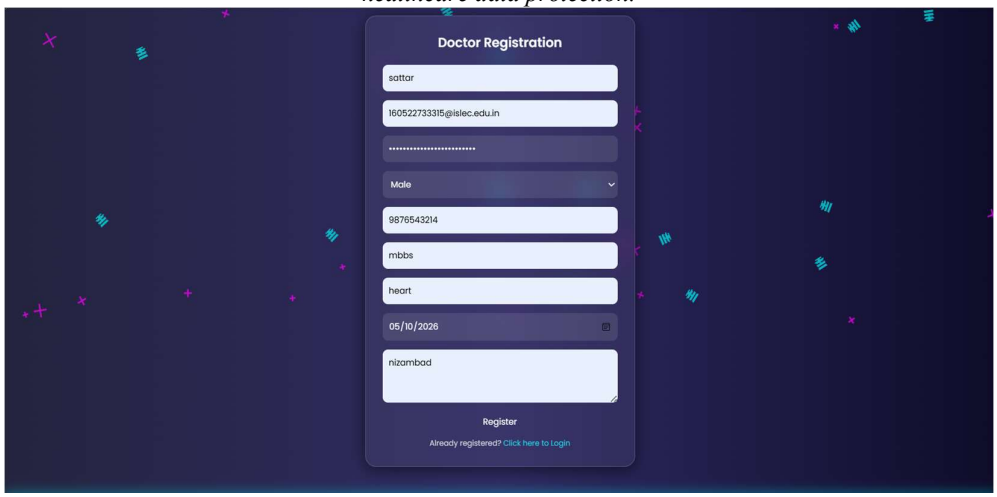

Fig. 2. Doctor Registration Form — Interface for new clinical user account creation with fields for name, email, password, gender, phone number, qualification, specialization, date, and address, followed by a register button and login option.

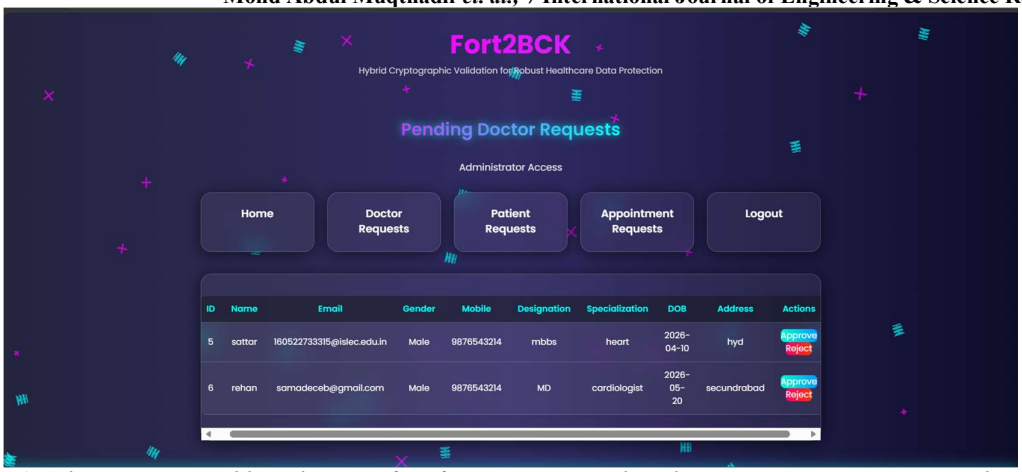

Fig. 3. Administrator Dashboard — Interface for managing pending doctor registration requests within the Fort2BCK system, showing applicant details such as ID, name, email, gender, mobile, designation, specialization, date of birth, and address, with options to approve or reject each request.

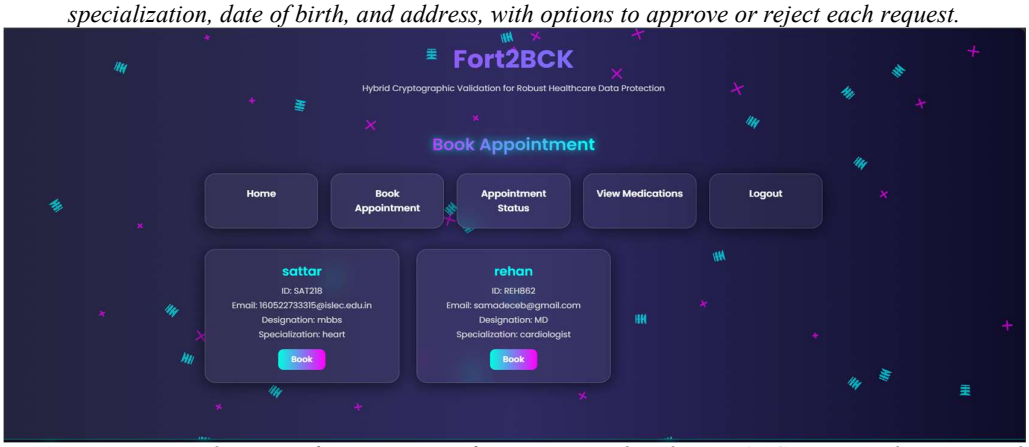

Fig. 4. Appointment Booking Interface — Patient-facing page within the Fort2BCK system showing available doctors with their ID, email, designation, and specialization, alongside options to book appointments securely through cryptographic validation

Fig. 5. Appointment Request Management — Administrator view within the Fort2BCK system showing pending patient appointment requests, including doctor and patient details, request time, and options to approve or reject each request for secure healthcare data handling.

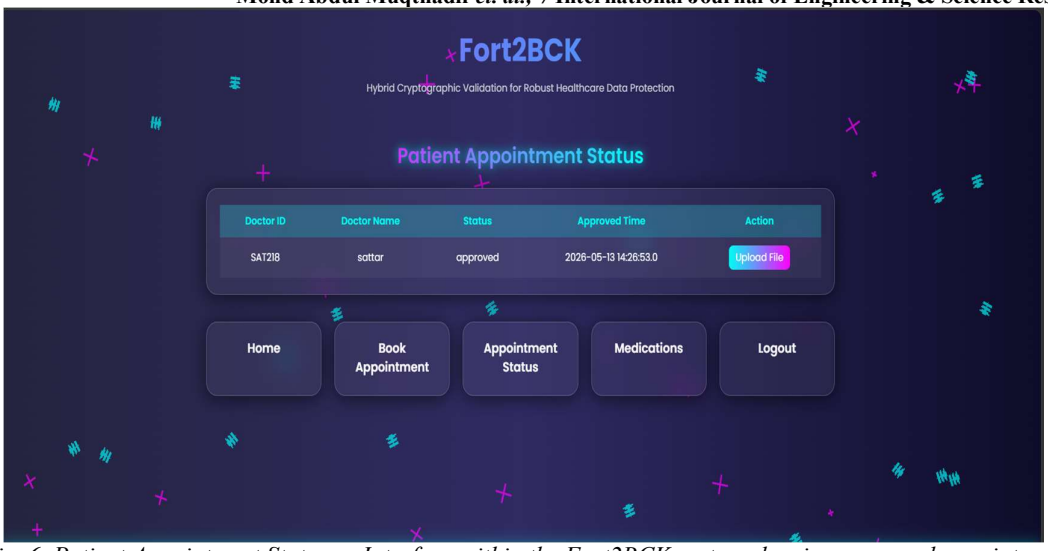

Fig. 6. Patient Appointment Status — Interface within the Fort2BCK system showing approved appointment details with doctor ID, doctor name, status, and approved time, along with an option for patients to securely upload files related to their visit.

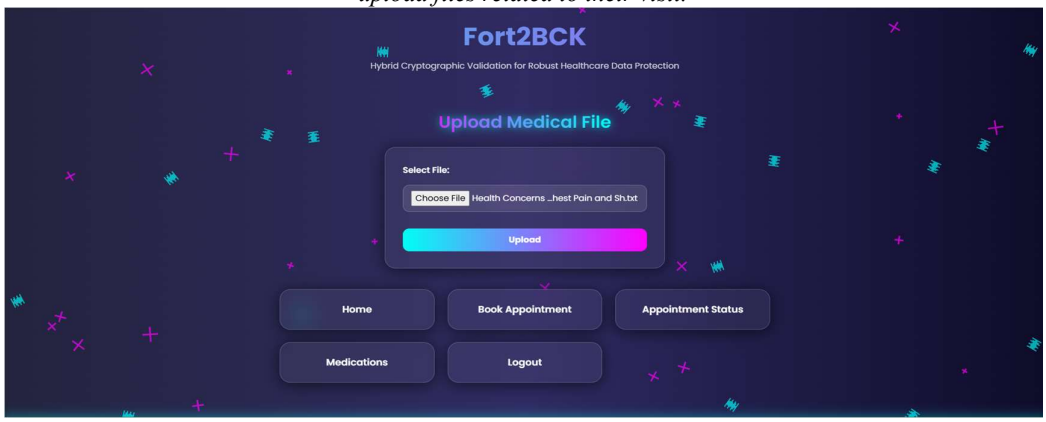

Fig. 7. Medical File Upload — Patient interface within the Fort2BCK system providing a secure form to select and upload medical documents, supported by navigation options for appointments,status tracking, medications, and logout.

Fig. 8. Doctor Dashboard — Fort2BCK interface displaying secure patient data management with encrypted records, RSA private key, and digital signature, alongside options for downloading files or sending them to the laboratory.

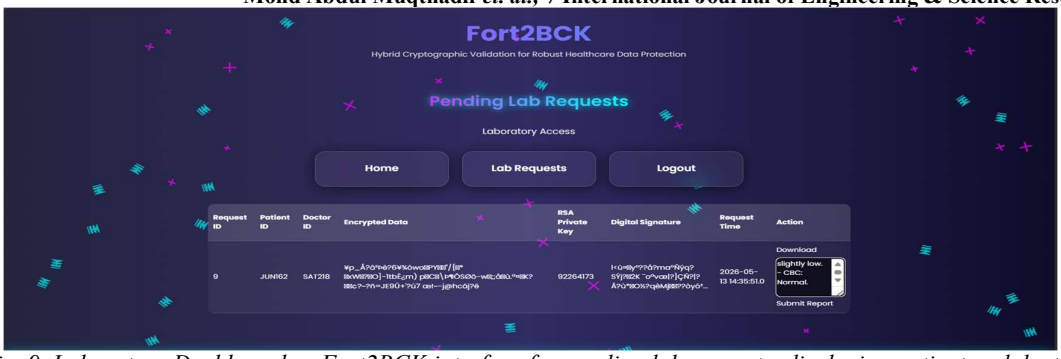

Fig. 9. Laboratory Dashboard — Fort2BCK interface for pending lab requests, displaying patient and doctor IDs, encrypted data, RSA private key, and digital signature, with options to download files and submit reports securely.

Fig. 10. Doctor Home Dashboard — Fort2BCK interface presenting approved patient requests with lab report status, report issued time, and medication entry fields, enabling doctors to securely prescribe treatments and save them within the system.

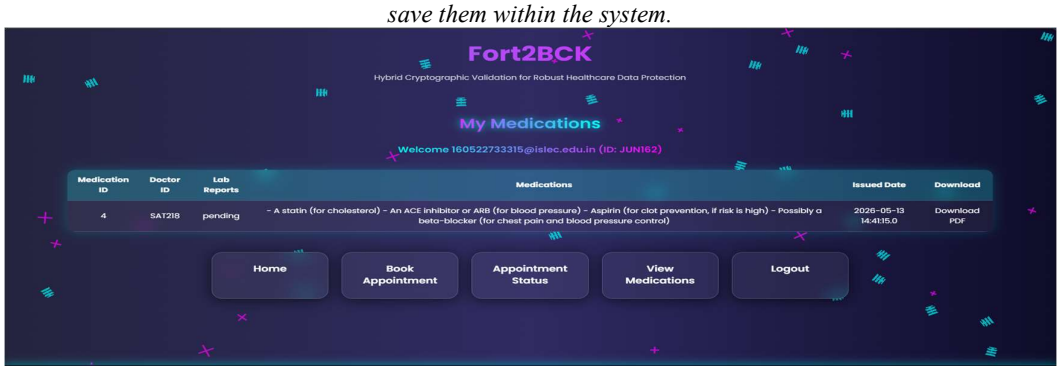

Fig. 11. Patient Medication Records — Fort2BCK interface displaying a patient's prescribed treatments with doctor ID, lab report status, detailed medication list, issued date, and secure download option, emphasizing cryptographic validation in healthcare data management.

CONCLUSION

In conclusion, the proposed block chain-based healthcare management system effectively ensures secure, transparent, and efficient handling of medical data through the integration of RSA encryption, SHA-256 hashing, and block chain technology. By dividing patient files into encrypted blocks and linking them with cryptographic hashes, the system maintains data integrity and immutability, preventing unauthorized access or tampering. The digital signature generation using Fort2Bck guarantees authentication and non-repudiation of medical records. The collaborative modules—Doctor, Patient, Administrator, and Laboratory—work together seamlessly to provide a trustworthy and decentralized healthcare ecosystem. Doctors can securely access patient reports, laboratories can process and upload verified results, and administrators manage approvals efficiently. The use of private key verification ensures that only authorized users can decrypt sensitive data, reinforcing privacy and compliance. Overall, the system successfully overcomes challenges in traditional healthcare management by introducing data confidentiality, traceability, and accountability. This project demonstrates how block chain and cryptographic techniques can revolutionize healthcare data exchange, fostering trust among all

participants while paving the way for more advanced, intelligent, and scalable healthcare innovations in the future.

VIII. FUTURE SCOPE

In the future, this block chain-based healthcare management system can be enhanced by integrating AI-driven predictive analytics to assist doctors in diagnosing diseases more accurately using patient medical histories and lab reports. The system can also include IoT-enabled medical devices that automatically update patient health data into the block chain in real time, improving data accuracy and reducing manual errors. Further enhancement can involve multi-chain interoperability, allowing data exchange across different healthcare block chains to ensure seamless coordination between hospitals and laboratories. Incorporating Zero-Knowledge Proofs (ZKP) can enhance privacy by enabling data verification without exposing sensitive information. Additionally, cloud-based scalability can support high-volume data storage and retrieval efficiently. The system can integrate mobile and wearable device compatibility for patient monitoring. Smart contracts can automate insurance claims and billing processes. Future updates could also include federated learning models for secure AI training on decentralized data. Moreover, enhanced user interfaces for accessibility, advanced encryption standards for better security, and integration with national health records can further elevate this project into a complete, intelligent, and globally scalable healthcare data management solution.

REFERENCES

[1] K. Ramar, P. V. Gopirajan, H. Shanmugasundaram, B. P. Andraju, and S. Baskar, "Digital Healthcare using Blockchain," *2022 1st Int. Conf. Comput. Sci. Technol. (ICCST 2022)*, pp. 651–655, 2022, doi: 10.1109/ICCST55948.2022.10040411.

[2] A. Cervera García and A. Goussens, "Cybersecurity and use of ICT in the health sector," *Aten. Primaria*, vol. 56, no. 3, p. 102854, 2024, doi: 10.1016/j.aprim.2023.102854.

[3] A. M. Udroiu, M. Dumitrache, and I. Sandu, "Improving the cybersecurity of medical systems by applying the NIST framework," *2022 14th Int. Conf. Electron. Comput. Artif. Intell. (ECAI 2022)*, pp. 1–7, 2022, doi: 10.1109/ECAI54874.2022.9847498.

[4] Z. Baruwa, S. Bhattacherjee, S. R. Chandnani, and Z. Zhu, "Social Media Perceptions of 51% Attacks on Proof-of-Work Cryptocurrencies: A Natural Language Processing Approach," pp. 1–23, 2023. [Online]. Available: http://arxiv.org/abs/2310.14307.

[5] Y. Wang and M. Tan, "Defense against Sybil attack in blockchain based on improved consensus algorithm," *2023 IEEE Int. Conf. Control. Electron. Comput. Technol. (ICCECT 2023)*, pp. 986–989, 2023, doi: 10.1109/ICCECT57938.2023.10140278.

[6] S. Yan, "Analysis on Blockchain Consensus Mechanism Based on Proof of Work and Proof of Stake," *Proc. – 2022 Int. Conf. Data Anal. Comput. Artif. Intell. (ICDACAI 2022)*, pp. 464–467, 2022, doi: 10.1109/ICDACAI57211.2022.00098.

[7] N. Ettaloui, S. Arezki, and T. Gadi, "An Overview of Blockchain-Based Electronic Health Record and Compliance with GDPR and HIPAA," in *Artificial Intelligence, Data Science and Applications*, 2024, pp. 405–412.

[8] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," *Proc. – 2016 2nd Int. Conf. Open Big Data (OBD 2016)*, pp. 25–30, 2016, doi: 10.1109/OBD.2016.11.

[9] K. Ito, K. Tago, and Q. Jin, "I-Blockchain: A Blockchain-Empowered Individual-Centric Framework for Privacy-Preserved Use of Personal Health Data," *Proc. – 9th Int. Conf. Inf. Technol. Med. Educ. (ITME 2018)*, pp. 829–833, 2018, doi: 10.1109/ITME.2018.00186.

[10] P. Verma, V. Tripathi, and B. Pant, "ZeroMedChain: Layer 2 Security and Zero-Knowledge Proof Integration for Decentralized Identity and Access Management in Healthcare," *Proc. 18th INDIACom 2024 – 11th Int. Conf. Comput. Glob. Dev.*, pp. 1023–1027, 2024, doi: 10.23919/INDIACom61295.2024.10498190.