AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(2) (2026)

A Hybrid Post-Quantum and Blockchain-Based Model for Tamper-Proof Healthcare Data Systems

K. Madhavi[1], Bandra Manohar[1], Musa Abdalla Hassan Daggag[1], Alimineti Rakesh[1], Shaik Rafi[1]

[1]Department of Computer Science and Engineering, [1]Sree Dattha Institute of Engineering and Science, Nagarjuna Sagar Road, Sheriguda, Ibrahimpatnam, Rangareddy Dist, 501510, Telangana, India.

ABSTRACT

Quantum-Resistant Blockchain for Secure Health Data is designed to tackle increasing security challenges in healthcare systems caused by outdated encryption methods and centralized data storage. In India, incidents of healthcare data breaches have risen significantly, including the 2021 breach of a government health database that exposed over 100 million records. With the rapid growth of digital health records, telemedicine, and e-governance, there is a critical need for quantum-resistant cryptographic solutions to protect patient information. As initiatives like the Ayushman Bharat Digital Mission (ABDM) advance digital healthcare ecosystems, combining blockchain with post-quantum security becomes essential for ensuring decentralized, tamper-proof, and future-ready data management. The primary objective of this work is to develop a secure and decentralized healthcare data system by integrating blockchain technology with quantum-resistant cryptographic mechanisms, ensuring data confidentiality, integrity, and support for machine learning-based diagnostics. Traditional healthcare data management systems rely on physical records, spreadsheets, or basic databases where patient information is manually entered and shared across departments. Such approaches often result in inefficiencies, delays, and weak access control. These systems are prone to human errors, document degradation, data redundancy, unauthorized access, limited historical tracking, absence of real-time analysis, and lack of transparency or auditability. This research is motivated by the shortcomings of manual and partially digital systems that cannot provide scalable and robust security. By leveraging blockchain and post-quantum cryptography, the proposed solution mitigates risks associated with future quantum attacks while ensuring secure communication, immutable records, and privacy-preserving data analysis within a tamper-resistant framework. Additionally, the system integrates machine learning models to analyze decrypted health data for diagnostic support and risk prediction. Advanced post-quantum cryptographic algorithms such as FALCON for digital signatures and KYBER for key encapsulation are employed to secure the system. Blockchain technology records all activities related to file access, uploads, and downloads, ensuring traceability, transparency, and resistance to data tampering.

Keywords: Quantum-Resistant Cryptography, Blockchain Technology, Secure Health Data, FALCON, KYBER, Digital Health Systems.

1. INTRODUCTION

The digital transformation of healthcare demands robust, secure, and intelligent systems for managing sensitive patient data. Traditional methods of file storage and communication are susceptible to breaches and lack transparency. This project proposes a next-generation secure healthcare framework that combines Post-Quantum Cryptography (FALCON, KYBER) for encryption, Blockchain for decentralized, immutable logging, and Machine Learning for predictive analysis of medical data. The goal is to create a complete, end-to-end solution for uploading, encrypting, sharing, analysing, and retrieving healthcare files in a secure and intelligent way.

Recently, hacker attacks on hospitals have become a significant concern. Hackers may steal patient data or implant malware within hospital systems, rendering the data inaccessible [1]. One of the most malicious attacks is ransomware, where hackers lock down critical patient and medical data on the hospital's servers and demand payment in exchange for restoring access [2]. Even if the hospital pays

the ransom, hackers often demand more money or fail to unlock the data. These types of attacks can occur even in well-structured hospital systems if, for example, operating system updates are neglected or malicious email attachments or links are mistakenly opened [3].

In particular, when a hospital needs to transfer a patient's medical information to another hospital due to relocation or deteriorating health, serious security issues can arise: An attacker may impersonate a hospital and send attachments or links containing malware to attack the internal servers of the hospital. (2) There could be privacy breaches where an attacker intercepts and steals patient medical information during the transfer between hospitals. (3) An attacker might disrupt communication between hospitals. To prevent such attacks, a robust security system for secure interaction between hospitals is essential [4].

To address these security challenges, we propose a new protocol system that incorporates blockchain technology. This proposed protocol provides a solution in cases where a hospital's internal system is compromised and server recovery is difficult by allowing the hospital to retrieve encrypted information from the blockchain. To securely transfer patient data and medical records between hospitals, the protocol records the relevant information on the blockchain and ensures that only verified institutions can interact by generating session keys for encryption. Additionally, when a patient wishes to transfer their treatment from one hospital to another, they often face the inconvenience of resubmitting insurance and identity verification documents. Our protocol addresses this issue by allowing insurance companies to be verified and registered on the blockchain, enabling them to access patient information and record the patient's insurance status securely [5]

2. LITERATURE SURVEY

Enaya et al [6]. explored blockchain applications in the IoT, focusing on security, automation, scalability, and data sharing. Industry-specific applications, including supply chain management, smart cities, and healthcare, highlight the potential of blockchains to optimize operations, ensure compliance, and foster innovation. Additionally, blockchain technology enables robust audit trails, enhances accountability, and reduces fraud in sensitive IoT applications, such as finance and healthcare. The synergy between blockchains and the IoT creates a secure and transparent platform for managing device interoperability and data exchange, fostering seamless communication between diverse IoT components. Furthermore, this paper discusses layer 2 scaling techniques and tokenization to address scalability, ownership, monetization, and cost challenges, providing practical solutions for real-world deployments. Future directions emphasize integrating blockchain systems with artificial intelligence (AI), machine learning (ML), and edge computing, offering groundbreaking capabilities to further revolutionize IoT ecosystems. By merging these advanced technologies, organizations can build secure, scalable, and intelligent systems to drive innovation and trust. Ohize et al. [7] presented a survey of the latest trends in the development of e-voting systems, focusing on the integration of blockchain technology as a promising solution to address various concerns in e-voting, including security, transparency, auditability, and voting integrity. They survey is important because existing survey articles do not cover the latest advancements in blockchain technology for e-voting, particularly as it relates to architecture, global trends, and current concerns in the developmental process. Thus, we address this gap by providing an encompassing overview of architectures, developments, concerns, and solutions in e-voting systems based on the use of blockchain technology. Specifically, a concise summary of the information necessary for implementing blockchain-based e-voting solutions is provided. Furthermore, we discuss recent advances in blockchain systems, which aim to enhance scalability and performance in large-scale voting scenarios. We also highlight the fact that the implementation of blockchain-based e-voting systems faces challenges, including cybersecurity risks, resource intensity, and the need for robust infrastructure, which must be addressed to ensure the scalability and reliability of these systems.

Taherdoost et al. [8] processed by utilizing blockchain technology. By systematically examining articles published from 2017 to 2022, this review addresses the existing gap by methodically discussing the state, research trends, and challenges of blockchain in medical data exchange. The number of articles on this issue has increased, reflecting the growing importance and interest in blockchain research for medical data exchange. Recent blockchain-based medical data sharing advances include safe healthcare management systems, health data architectures, smart contract frameworks, and encryption approaches. The evaluation examines medical data encryption, blockchain networks, and how the Internet of Things (IoT) improves hospital workflows. The findings show that blockchain can improve patient care and healthcare services by securely sharing data.

Li et al. [9] provided a secure execution environment for SQLCipher, isolating all sensitive operations of healthcare data from the untrusted environment to ensure the confidentiality and integrity of the data. Additionally, we design a TEE-empowered session key generation protocol that enables secure authentication and key sharing for both parties involved in data sharing. Finally, we implement TrustHealth using Hyperledger Fabric and ARM TrustZone. Through security and performance evaluation, TrustHealth is shown to securely process massive encrypted data flows at a rate of 5000 records per second, affirming the feasibility of our proposed scheme. We believe that TrustHealth offers valuable guidelines for the design and implementation of similar systems, providing a valuable contribution to ensuring the privacy and security of eHealth systems. Ali et al. [10] proposed a permissions-based blockchain framework for scalable and secure healthcare systems, integrating hybrid deep learning models. The framework ensures that only authorized entities can access and modify sensitive health information, preserving patient privacy while facilitating seamless data sharing and collaboration among healthcare providers. Additionally, the hybrid deep learning models enable real-time analysis of large-scale healthcare data, facilitating timely diagnosis, treatment recommendations, and disease prediction. The integration of blockchain and hybrid deep learning presents numerous benefits, including enhanced scalability, improved security, interoperability, and informed decision making in healthcare systems. However, challenges such as computational complexity, regulatory compliance, and ethical considerations need to be addressed for successful implementation. By harnessing the potential of blockchain and hybrid deep learning, healthcare systems can overcome traditional limitations, promoting efficient and secure data management, personalized patient care, and advancements in medical research. The proposed framework lays the foundation for a future healthcare ecosystem that prioritizes scalability, security, and improved patient outcomes.

Ngabo et al. [11] provided security countermeasures against medical data mining threats, which are generated from the sensing layer (a human wearable device) and storage of data in the cloud database of internet of things (IoT). Therefore, we propose a public-permissioned blockchain security mechanism using elliptic curve crypto (ECC) digital signature that that supports a distributed ledger database (server) to provide an immutable security solution, transaction transparency and prevent the patient records tampering at the IoTs fog layer. The blockchain technology approach also helps to mitigate these issues of latency, centralization, and scalability in the fog model. Alabdulatif et al. [12] integrated modern technologies to alleviate security issues in the smart healthcare system. Therefore, in this article, we conduct a comprehensive review of the various most recent security challenges and their countermeasures in the smart healthcare environment. In addition, an artificial intelligence (AI) and blockchain-based secure architecture is proposed as a case study to analyse malware and network attacks on wearable devices. The proposed architecture is evaluated using various performance metrics such as blockchain scalability, accuracy, and dynamic malware analysis. Lastly, we highlight different open issues and research challenges facing smart healthcare systems.

Li et al. [13] explored methods for defending against quantum computer attacks. Among the methods currently developed, quantum key distribution is a technology that uses the principles of quantum mechanics to distribute keys. Post-quantum encryption algorithms are encryption methods that rely on

mathematical challenges that quantum computers cannot solve quickly to ensure security. In this study, an integrated review of post-quantum encryption algorithms is conducted from the perspective of traditional cryptography. First, the concept and development background of post-quantum encryption are introduced. Then, the post-quantum encryption algorithm Kyber is studied. Finally, the achievements, difficulties and outstanding problems in this emerging field are summarized, and some predictions for the future are made. Taralunga et al. [14] proposed a new healthcare concept centered on the patient. Patients' real-time remote continuous health monitoring, remote diagnosis, treatment, and therapy is possible in an mHealth system. However, major limitations include the transparency, security, and privacy of health data. One possible solution to this is the use of blockchain technologies, which have found numerous applications in the healthcare domain mainly due to theirs features such as decentralization (no central authority is needed), immutability, traceability, and transparency. We propose an mHealth system that uses a private blockchain based on the Ethereum platform, where wearable sensors can communicate with a smart device (a smartphone or smart tablet) that uses a peer-to-peer hypermedia protocol, the InterPlanetary File System (IPFS), for the distributed storage of health-related data. Moraes Rossetto et al [15]. presented an architecture to ensure the privacy of health-related data, which are stored and shared within a blockchain network in a decentralized manner, through the use of encryption with the RSA, ECC, and AES algorithms. Evaluation tests were performed to verify the impact of cryptography on the proposed architecture in terms of computational effort, memory usage, and execution time. The results demonstrate an impact mainly on the execution time and on the increase in the computational effort for sending data to the blockchain, which is justifiable considering the privacy and security provided with the architecture and encryption.

3. PROPOSED METHODOLOGY

This research presents a comprehensive and secure healthcare data management system by leveraging blockchain technology integrated with post-quantum cryptographic techniques. The primary goal of this research is to ensure the privacy, integrity, and immutability of electronic health records (EHRs) in an era where quantum computing poses a real threat to conventional encryption methods. The system facilitates secure communication and data exchange between patients and doctors, ensuring that all sensitive health information remains protected from unauthorized access and tampering. By using smart contracts on a blockchain network, this research eliminates the need for centralized control, thereby reducing the risk of data breaches and administrative manipulation.

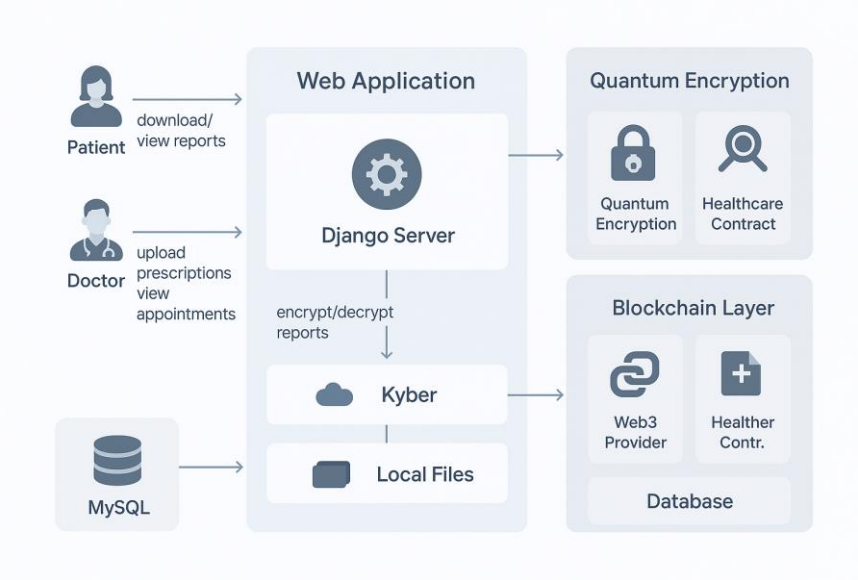

Fig. 1: Proposed system architecture.

The application developed under this research is built using Django as the backend framework and integrates Ethereum blockchain smart contracts using the Web3.py interface. Post-quantum algorithms

such as Kyber and Falcon are incorporated for encryption, decryption, and key exchange, ensuring resistance against quantum attacks. When a patient uploads a medical report, the file is first encrypted using quantum-resistant encryption and then securely stored, while the transaction metadata is immutably logged on the blockchain. Doctors can view these reports and generate prescriptions, which are again encrypted and stored securely. Patients can later access their prescriptions and download reports, all while maintaining the confidentiality and integrity of the data.

Quantum Encryption Layer

The Quantum Encryption Layer provides advanced cryptographic protection for sensitive healthcare data such as medical reports and prescriptions. Traditional encryption algorithms are vulnerable to future quantum computers, which can break classical keys using algorithms like Shor's. To counter this, the system uses post-quantum cryptographic methods specifically the Kyber key encapsulation mechanism to generate quantum-resistant shared keys. These keys are used to encrypt and decrypt files securely before they are stored or transmitted. In this architecture, encryption happens inside the Django server immediately after a doctor uploads a medical report or prescription. The Kyber algorithm generates a unique pair of public–private keys and establishes a secure shared secret. This shared secret key is then used for symmetric file encryption, ensuring that even if attackers intercept the files, the data remains unreadable. Since decryption uses the same quantum-safe key, only authorized users patient or doctor can access the original information. The Quantum Encryption Layer works in coordination with the blockchain layer by storing only encrypted file references (not the actual files) on the blockchain. This maintains confidentiality while leveraging blockchain's immutability. The encryption layer ensures that even if blockchain data is publicly visible, the sensitive medical information cannot be deciphered. Thus, the system achieves secure end-to-end encryption using quantum-resistant techniques.

1. Users upload medical reports or prescriptions.
2. Django server reads the file.
3. The Kyber algorithm generates quantum-safe encryption keys.
4. Symmetric encryption is applied using the generated key.
5. The encrypted file is saved in local storage.
6. Encrypted filename is stored on blockchain.
7. During download, Django decrypts using the same Kyber key.

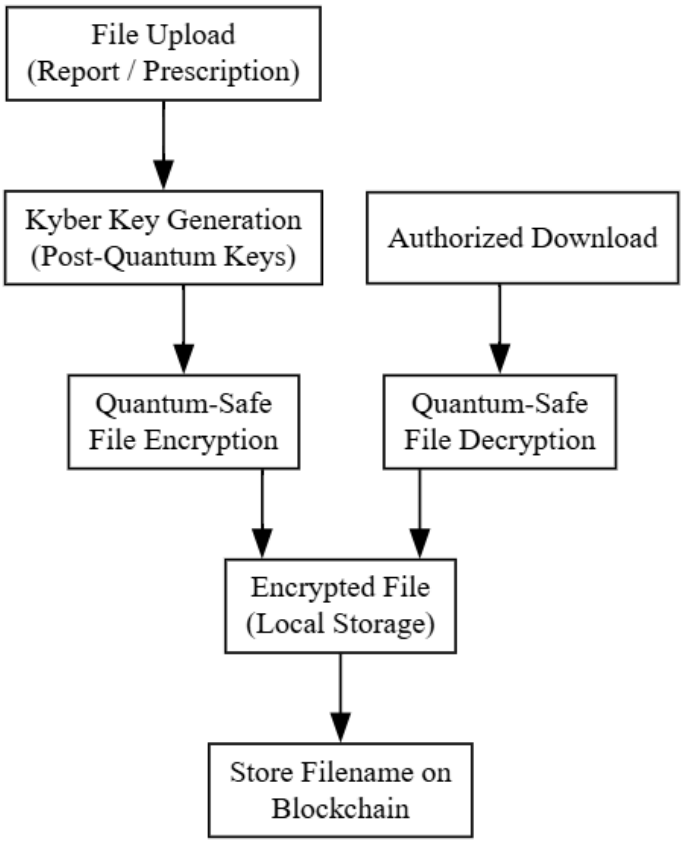

Fig. 2: Quantum encryption layer architecture.

4. IMPLEMENTATION DESCRIPTION

The implementation of the proposed Quantum-Secured Blockchain-Enabled Healthcare System is carried out using Django as the backend framework, Ethereum blockchain smart contracts for storing immutable EHR metadata, and a hybrid Kyber + custom quantum encryption module for post-quantum-secure file encryption. The system ensures that medical reports, prescriptions, and appointment data are securely transmitted, stored, and accessed only by authorized users. The implementation is structured into modules such as user management, appointment handling, quantum encryption, blockchain interfacing, and doctor–patient communication workflows.

1. Django Backend Architecture

The Django framework acts as the central orchestrator for all user requests. It handles:

- Patient and doctor registration
- Login authentication
- Viewing available doctors
- Booking appointments
- Uploading medical reports
- Generating prescriptions
- Viewing encrypted files

Each URL request is mapped to a corresponding view function where the logic is executed. Django manages templates on the frontend and integrates seamlessly with the quantum encryption module and blockchain contract.

2. Blockchain Smart Contract Integration

A deployed Ethereum smart contract (ABI + address provided in the project) maintains all critical, tamper-proof data:

- User registration details

- EHR metadata (patient, doctor, disease, report filename, date)
- Prescription updates

The backend connects to the blockchain using Web3.py. Key operations include:

- saveUser() - stores new user data
- saveEhr() - stores encrypted report metadata during booking
- updatePrescription() - stores encrypted prescription details
- getUserCount() and other getters fetch user/EHR data

The contract ensures immutability and a transparent audit trail.

3. Quantum-Safe Encryption Engine

This module performs all secure file operations using Kyber-based quantum encryption. When a user uploads a report or a doctor uploads a prescription:

1. A quantum-safe symmetric key is generated using computeQuantumKeys().
2. The file is encrypted through quantumEncryptMessage().
3. The encrypted file is stored in the system directory.
4. When a doctor or patient retrieves the file, it is decrypted using quantumDecryptMessage().
5. Key exchange is verified using exchangeKeys() before sensitive access.

This ensures confidentiality even against future quantum attacks giving your system a massive security flex.

4. File Handling and Secure Storage

All files (reports and prescriptions) are stored only after encryption in: HealthcareApp/static/files/

Before saving, the system checks if a filename already exists and replaces it if necessary. Files never reach the blockchain directly only their metadata is uploaded, ensuring efficiency and security.

5. Appointment Booking Workflow

When a patient books an appointment:

1. They choose a doctor from the blockchain-fetched list.
2. They upload a medical report.
3. Django reads the file, encrypts it via quantum module.
4. The encrypted file is stored locally.
5. Blockchain's saveEhr() function stores metadata like:
    - Patient
    - Doctor
    - Disease
    - Encrypted filename
    - Prescription placeholder
    - Date
6. The appointment is confirmed, and a transaction receipt is shown.

This ensures every appointment is securely registered and tamper-proof.

6. Doctor's Appointment Dashboard

When a doctor logs in, they can:

- View all appointments assigned to them
- Access encrypted medical reports
- Download decrypted versions
- Generate prescriptions

The system only shows appointments where exchangeKeys(patient, doctor) returns True, ensuring that only authenticated doctor–patient pairs can communicate.

7. Prescription Generation Workflow

Doctors generate prescriptions through:

1. Opening an appointment.
2. Entering prescription details.
3. Uploading prescription file (PDF/image).
4. File gets encrypted using quantumEncryptMessage().
5. Blockchain's updatePrescription() stores:
    - Prescription text
    - Encrypted file name

The patient can then download the file, where the system performs safe decryption.

8. Patient Dashboard Implementation

Patients get access to:

- Their appointments
- Uploaded reports
- Doctor prescriptions
- Downloadable encrypted files

The system dynamically splits the blockchain-stored prescription string (text#filename) to show both text and file link.

9. Data Structures and Global Lists

Two global lists maintain fast access without repeated blockchain calls:

- usersList - cached list of registered users
- prescriptionList - cached EHR metadata

Both lists get updated immediately after every blockchain transaction.

10. Security & Validation Implementation

Security mechanisms include:

- Quantum-safe hybrid encryption for all files
- Blockchain for ensuring tamper-proof data
- Role-based access control (patient vs doctor)
- File overwrite checks
- User existence checks before registration
- Decryption allowed only after key exchange verification

5. CONCLUSION

The proposed healthcare framework, which combines quantum-resistant cryptography with blockchain technology, provides a significant improvement in securing and managing electronic health records. While conventional cryptographic techniques such as RSA and AES remain effective against classical threats, they are susceptible to attacks from emerging quantum computing technologies. This system addresses those risks by implementing post-quantum algorithms like Kyber for secure key exchange and Falcon for encryption and decryption processes. These advanced algorithms are designed to withstand known quantum-based attacks, ensuring long-term protection of sensitive patient information. Furthermore, the incorporation of blockchain technology guarantees data integrity and transparency by maintaining immutable records, thereby reducing the risks associated with centralized storage and unauthorized modifications. Smart contracts are utilized to automate and secure user interactions and data transactions, strengthening system trust and reliability. Overall, the integration of these cutting-edge technologies results in a practical, scalable, and highly secure solution tailored for modern healthcare data management systems.

REFERENCES

[1] Zhang, P.; Han, W.; Liu, Q. Research on Predicting the Mental Health of College Students with Prediction Models based on Big Data Technology. IEIE Trans. Smart Process. Comput. 2024, 13, 393–401.
[2] Yu, P. Design of a Blockchain based Data Security Guarantee System for Logistics Systems. IEIE Trans. Smart Process. Comput. 2024, 13, 402–413.
[3] Cha, H.; Kim, I.K.; Kim, T. Using a random forest to predict quantized reuse distance in an SSD write buffer. Computing 2024, 106, 3967–3986.
[4] Ryu, J.; Kang, D.; Lee, H.; Kim, H.; Won, D. A secure and lightweight three-factor-based authentication scheme for smart healthcare systems. Sensors 2024, 20, 7136.
[5] Masud, M.; Gaba, G.S.; Choudhary, K.; Hossain, M.S.; Alhamid, M.F.; Muhammad, G. Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare. IEEE Internet Things J. 2021, 9, 2649–2656.
[6] Enaya A, Fernando X, Kashef R. Survey of Blockchain-Based Applications for IoT. Applied Sciences. 2025; 15(8):4562. https://doi.org/10.3390/app15084562
[7] Ohize, H.O., Onumanyi, A.J., Umar, B.U. et al. Blockchain for securing electronic voting systems: a survey of architectures, trends, solutions, and challenges. Cluster Comput **28**, 132 (2025). https://doi.org/10.1007/s10586-024-04709-8
[8] Taherdoost H. The Role of Blockchain in Medical Data Sharing. Cryptography. 2023; 7(3):36. https://doi.org/10.3390/cryptography7030036
[9] Li J, Luo X, Lei H. TrustHealth: Enhancing eHealth Security with Blockchain and Trusted Execution Environments. Electronics. 2024; 13(12):2425. https://doi.org/10.3390/electronics13122425
[10] Ali A, Ali H, Saeed A, Ahmed Khan A, Tin TT, Assam M, Ghadi YY, Mohamed HG. Blockchain-Powered Healthcare Systems: Enhancing Scalability and Security with Hybrid Deep Learning. Sensors. 2023; 23(18):7740. https://doi.org/10.3390/s23187740
[11] Ngabo D, Wang D, Iwendi C, Anajemba JH, Ajao LA, Biamba C. Blockchain-Based Security Mechanism for the Medical Data at Fog Computing Architecture of Internet of Things. Electronics. 2021; 10(17):2110. https://doi.org/10.3390/electronics10172110
[12] Alabdulatif A, Khalil I, Saidur Rahman M. Security of Blockchain and AI-Empowered Smart Healthcare: Application-Based Analysis. Applied Sciences. 2022; 12(21):11039. https://doi.org/10.3390/app122111039
[13] Li S, Chen Y, Chen L, Liao J, Kuang C, Li K, Liang W, Xiong N. Post-Quantum Security: Opportunities and Challenges. Sensors. 2023; 23(21):8744. https://doi.org/10.3390/s23218744
[14] Taralunga DD, Florea BC. A Blockchain-Enabled Framework for mHealth Systems. Sensors. 2021; 21(8):2828. https://doi.org/10.3390/s21082828
[15] de Moraes Rossetto AG, Sega C, Leithardt VRQ. An Architecture for Managing Data Privacy in Healthcare with Blockchain. Sensors. 2022; 22(21):8292. https://doi.org/10.3390/s22218292