Journal of Theoretical and Applied Information Technology
31st December 2025. Vol.103. No.24

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SECURING HEALTHCARE RECORDS: A BLOCKCHAIN-BASED APPROACH FOR DATA INTEGRITY AND ACCESS CONTROL

IKRAM BEN ABDEL OUAHAB[1], LOTFI ELAACHAK[2], YASSER ALLUHAIDAN[3], AND MOHAMMED BOUHORMA[4]

[1,2,4] DIS Team, C3S laboratory, Computer Science Engineering Department, Faculty of Sciences and Techniques of Tangier, University Abdelmalek Essaadi, Morocco

[3] HUMAIN, Cybersecurity Strategy & Architecture, Saudi Arabia

E-mail: [1]ibenabdelouahab@uae.ac.ma, [2]lelaachak@uae.ac.ma, [3]y.alluhaidan@gmail.com
[4]mbouhorma@uae.ac.ma

ABSTRACT

The management of medical records presents significant challenges in the healthcare sector, with traditional centralized systems plagued by vulnerabilities such as cyberattacks, unauthorized access, and data breaches. These issues compromise the confidentiality, integrity, and accessibility of sensitive patient information, further exacerbated by the increasing complexity and volume of healthcare data. This paper proposes a blockchain-based framework leveraging Ethereum's decentralized architecture and the InterPlanetary File System (IPFS) for distributed storage to address these challenges. Smart contracts, implemented in Solidity, automate critical processes such as patient registration, access control, and record updates, ensuring traceability and eliminating intermediaries. Sensitive medical data is encrypted before storage on IPFS, with only cryptographic hashes stored on-chain to reduce storage overhead while maintaining data integrity. Decentralized authentication mechanisms, such as Ethereum wallets and cryptographic keys, enhance security and usability. This approach empowers patients with full control over their data and real-time access management. The system's scalability, transparency, and patient-centric design provide a robust alternative to traditional models, paving the way for advancements in healthcare data management and beyond.

Keywords: *Blockchain Technology, Medical Record Management, Data Security, Smart Contracts, InterPlanetary File System (IPFS)*

1. INTRODUCTION

The management of medical records is a critical issue in the healthcare sector, as traditional centralized systems frequently encounter significant challenges in data security, privacy, and accessibility. Centralized databases are highly vulnerable to cyberattacks, unauthorized access, and data breaches, jeopardizing the confidentiality and integrity of sensitive patient information. Moreover, these systems often lack effective mechanisms for tracking data modifications or providing transparency regarding access and changes to medical records. The growing complexity and volume of healthcare data further underscore the need for innovative, secure, and patient-centric solutions.

To address these challenges, this paper proposes a blockchain-based system for secure medical record management. By leveraging Ethereum's decentralized blockchain and utilizing IPFS for distributed storage, the proposed framework ensures that patient data remains secure, immutable, and transparent. Smart contracts, developed in Solidity, automate key processes such as patient registration, access control, and record updates, eliminating intermediaries and ensuring all actions are traceable. Sensitive medical data is encrypted before being stored on IPFS, with only the file hashes stored on the blockchain to preserve data integrity while minimizing on-chain storage requirements. Decentralized authentication methods, such as Ethereum wallets or cryptographic keys, provide secure and user-friendly access, further strengthening the system's security.

This paper makes two key contributions: first, it introduces a secure and transparent solution for medical record management, enabling patients to maintain full control over their data and dynamically grant or revoke access to healthcare providers. Second, the system offers a scalable and efficient alternative to traditional centralized approaches, addressing critical issues such as data breaches, unauthorized access, and lack of transparency. By integrating blockchain, smart contracts, and IPFS, this framework presents a novel approach to overcoming the limitations of current medical record systems and supports the transition toward decentralized healthcare ecosystems.

Blockchain technology's decentralized, immutable, and transparent nature provides a promising foundation for addressing these challenges. It ensures the confidentiality, integrity, and traceability of medical data while offering patients and healthcare providers secure and efficient access. Despite its potential, the adoption of blockchain in healthcare faces challenges such as scalability, latency, user accessibility, and integration with existing systems. This paper explores these challenges and proposes solutions to facilitate the adoption of blockchain technology in healthcare.

The proposed blockchain-based medical record management system represents a significant improvement over traditional centralized models, addressing critical concerns related to security, privacy, and patient autonomy. Beyond medical record management, the solution has the potential to transform other areas of healthcare, including pharmaceutical supply chains, insurance claim processing, and clinical trials, ultimately contributing to a more secure, transparent, and efficient healthcare ecosystem.

In this paper, we propose a blockchain-based decentralized application (DApp) that integrates smart contracts written in Solidity and deployed on the Ethereum blockchain. This application facilitates transparent and tamper-proof storage and sharing of medical records. A native front-end application provides a user-friendly interface for interacting with the blockchain, ensuring accessibility without compromising security.

By examining the intersection of blockchain technology and healthcare, this research aims to deliver an innovative, scalable, and secure approach to medical record management, addressing the growing demand for data protection, transparency, and decentralized healthcare systems. This study highlights blockchain's potential to redefine medical data management and lays the groundwork for future advancements in secure digital healthcare solutions.

2. CONTRIBUTION

This paper introduces a groundbreaking approach to medical record management by leveraging blockchain technology, significantly enhancing security, transparency, and control over sensitive data compared to traditional solutions. Centralized medical record systems are prone to vulnerabilities such as data breaches, unauthorized access, and single points of failure. Additionally, these systems often lack robust mechanisms for tracking modifications or ensuring data immutability, leading to potential disputes over data integrity and privacy violations.

The proposed solution addresses these limitations by integrating Ethereum blockchain and IPFS, enabling decentralized storage and management of medical records. Its novelty lies in using smart contracts to automate and secure critical processes such as patient registration, access control, and record updates, eliminating reliance on intermediaries and ensuring trust in the system. Unlike traditional models, where patients have limited control over their data, this solution empowers individuals with full ownership of their medical records, allowing them to dynamically grant or revoke access and trace all actions performed on their data.

Moreover, by employing IPFS for file storage and storing only file hashes on the blockchain, the solution balances data security and scalability, addressing blockchain's limited on-chain storage capacity. Decentralized authentication mechanisms, such as cryptographic keys and Ethereum wallets, further enhance security by eliminating vulnerabilities associated with traditional username-password systems.

In essence, this project represents a paradigm shift in medical record management, offering a secure, transparent, and patient-centric alternative that addresses the critical flaws of traditional systems while meeting the growing demand for decentralized and trustworthy healthcare solutions.

3. LITERATURE REVIEW

The secure management of medical records is a critical challenge in the healthcare industry, where data breaches, unauthorized access, and human errors threaten patient privacy and data integrity.

Traditional centralized systems often fail to provide the necessary security guarantees, exposing sensitive medical information to potential vulnerabilities. These shortcomings are particularly concerning in an era where healthcare increasingly relies on interconnected digital systems.

Healthcare applications has emerged as a significant target for cybercriminals due to the high value of medical records, both on the black market and for malicious purposes. Data breaches involving medical records have become increasingly prevalent over the past decade, resulting in the exposure of millions of patient records. According to recent reports, since 2009, the United States alone has witnessed 5,478 breaches, compromising over 423 million medical records. Annual statistics reveal a worrying trend in the volume of breaches within the healthcare sector. In 2020, the number of breaches reached 821, affecting a staggering 47 million records, marking one of the highest incidences in recent years. Although the frequency of breaches saw a decline in 2021 (757 breaches) and 2022 (562 breaches), the scale of records compromised remained alarmingly high, with 47.6 million records breached in 2022 alone [1].

The 2023 IBM Security Cost of a Data Breach Report reveals that the global average cost of a data breach has risen to $4.45 million, or $165 per record [2]. The United States experienced the highest average breach costs at $9.48 million, marking a 0.4% increase from the previous year. Notably, data breach costs have surged by 15% since 2020. The report, compiled by the Ponemon Institute, analyzed data from 553 organizations across 16 countries and included interviews with thousands of individuals. The breaches studied occurred between March 2022 and March 2023 [3].

Another major incident in 2024 involved Change Healthcare, a prominent healthcare technology company, which experienced a ransomware attack affecting over 100 million individuals and significantly disrupting healthcare services across multiple regions [4]. Additionally, a significant breach occurred in Scotland's NHS Dumfries & Galloway, where a cyber-attack led to the exposure of personal and medical data of more than 100,000 individuals. Despite refusing to comply with ransom demands, the organization faced the publication of stolen data by the cybercriminal group Inc Ransom on the dark web [5].

Moreover, the COVID-19 pandemic induced a marked acceleration in the digital transformation of healthcare services, which, in turn, amplified the cybersecurity risks faced by medical organizations. As healthcare institutions rapidly transitioned to remote work, expanded telemedicine services, and digitized patient records, the threat landscape expanded, offering increased opportunities for cyber adversaries to exploit vulnerabilities [6], [7].

Below are some significant breaches that occurred during the pandemic:

In 2020, UCLA Health experienced a breach impacting approximately 3.7 million individuals, triggered by a phishing attack that compromised a staff member's account. The breach exposed sensitive personal health information, including medical records and insurance details. This incident underscored the vulnerabilities introduced by the expanded remote operations and the increased reliance on digital communications within healthcare environments during the pandemic [8].

In 2020, Cognizant, a major IT services provider for healthcare organizations, fell victim to a ransomware attack attributed to the Maze ransomware group. The attack resulted in a significant disruption of healthcare services, including the loss of access to critical systems and the exposure of patient data. The breach highlighted the vulnerabilities of healthcare service providers in a landscape where remote operations and digital health tools were being rapidly deployed to meet the pandemic's demands [9], [10], [11].

During the pandemic, the Netherlands witnessed a sharp increase in telemedicine-related data breaches, including one incident in which hackers gained access to over 1.1 million patient records from various healthcare institutions. This breach exploited security gaps in newly implemented telehealth platforms, emphasizing the importance of robust cybersecurity measures in securing sensitive health data during a period of rapid technological adoption in healthcare systems [12].

Throughout the COVID-19 period, the U.S. healthcare sector was subjected to a persistent wave of ransomware attacks, which took advantage of the operational stress imposed on healthcare providers. Key incidents included attacks on prominent hospital chains, such as Universal Health Services (UHS), that led to the compromise of patient data and operational disruption. These incidents highlighted the vulnerabilities of critical healthcare infrastructure and the increasingly sophisticated tactics used by threat actors, who leveraged the pandemic to launch highly targeted ransomware campaigns [13], [14].

These incidents collectively illustrate the heightened cybersecurity challenges faced by healthcare organizations during the COVID-19 pandemic [15], [16]. The rapid deployment of remote healthcare solutions, including telemedicine and electronic health records, created an expanded attack surface for adversaries to exploit. Moreover, the shift to remote work and increased reliance on digital tools underscored the need for more resilient cybersecurity frameworks within the healthcare sector. These breaches exemplify the criticality of integrating robust cybersecurity practices and advanced threat detection mechanisms in the face of an ever-evolving cyber threat landscape.

Traditional healthcare systems predominantly use centralized databases, which are prone to data breaches and administrative inefficiencies. Blockchain-based alternatives address these issues but often lack the scalability or seamless user experience required for widespread adoption. The usual implementation of blockchain applications [17], particularly for transaction validation, is through web applications rather than desktop apps. Web apps provide seamless connectivity with wallets like MetaMask, leveraging browser extensions for efficient transaction handling. This approach ensures better feasibility due to standard APIs and broader user adoption of web-based tools [18].

Here are some existing blockchain-based solutions include:

MedRec [19] : A blockchain system designed to manage medical records while ensuring patient control over their data.

Patientory [20]: A healthcare-focused DApp leveraging blockchain and IPFS for data storage and patient-centric control.

HealthChain [21]: A cross-platform solution integrating blockchain with modular accessibility for healthcare providers and patients.

4. MATERIALS AND METHODS

The implementation of the proposed solution involves a robust and carefully selected set of technologies to address the challenges of secure medical record management. Each component has been chosen to ensure optimal performance, security, and friendly user experience. The following technologies will be utilized: Ethereum blockchain, Solidity for Smart contracts, IPFS, and Python for the front-end.

4.1 Electronic medical records (EMRs)

Electronic Medical Records (EMRs) represent the digitized equivalent of traditional paper-based patient records, systematically maintained within healthcare institutions. These records encompass a comprehensive spectrum of patient data, including detailed medical history, diagnostic findings, prescribed treatments, medication regimens, immunization records, laboratory results, and imaging studies. As a cornerstone of modern healthcare, EMRs are instrumental in facilitating data-driven clinical decision-making, ensuring continuity of care, and improving the overall quality of patient management [22], [23].

The primary significance of EMRs lies in their ability to enhance operational efficiency and healthcare delivery through centralized access to patient data. This centralization enables healthcare providers to retrieve real-time patient information, reducing delays and redundancies in treatment. Advanced functionalities of EMR systems include clinical decision support (CDS) tools, which leverage embedded algorithms to provide diagnostic recommendations, flag potential drug interactions, and generate alerts for preventive care, such as screenings and vaccination reminders. Additionally, EMRs enable the seamless integration of administrative processes, such as billing systems, appointment scheduling, and resource management, thereby reducing clerical errors and administrative overhead.

Despite their widespread adoption, traditional EMR systems [24] are often implemented within centralized architectures, making them inherently vulnerable to various technical and security challenges. Centralized databases pose significant risks of cyberattacks, unauthorized access, and data breaches, threatening the confidentiality, integrity, and availability of sensitive patient information. Furthermore, these systems frequently lack robust mechanisms for audit trails, making it difficult to track modifications to records or validate data authenticity. The reliance on central points of control also exposes EMRs to risks of single-point failures, which can disrupt critical healthcare operations [25].

Given these limitations, there is a pressing need for innovative solutions that address the security, privacy, and scalability concerns associated with EMRs [17], [26]. Emerging technologies, such as blockchain, offer a transformative potential to redefine medical record management by introducing decentralized, immutable, and transparent systems. Such advancements ensure that

patient data remains secure, auditable, and accessible while empowering individuals with greater control over their medical records.

4.2 InterPlanetary File System (IPFS)

The InterPlanetary File System (IPFS) is a decentralized protocol designed for file storage and sharing, aiming to enhance the web's speed, security, and openness [27]. Unlike traditional centralized storage systems, IPFS employs a peer-to-peer network architecture, distributing data across multiple nodes. This decentralized approach eliminates single points of failure, significantly enhancing data resilience, availability, and accessibility.

IPFS offers several key advantages. Its decentralized architecture distributes files across a global network of nodes, minimizing the risk of data loss and ensuring continuous accessibility, even in the event of node failures. The protocol ensures data integrity through the use of cryptographic hashes, which uniquely identify files and provide a tamper-evident mechanism to detect any modifications. Additionally, IPFS enhances efficiency by enabling direct content sharing between users through content-based addressing, bypassing the need for centralized intermediaries and improving both scalability and file distribution speed.

Large medical files (e.g., imaging scans or detailed reports) will be stored on IPFS, a distributed file system, because of the size limitations of on-chain storage. IPFS ensures data redundancy and efficient retrieval while maintaining security. Only the hashes of these files will be stored on the Ethereum blockchain, ensuring data integrity and reducing blockchain storage costs.

Pinata is a service that facilitates file management on IPFS. It allows files to be "pinned" on the IPFS network, ensuring that they remain accessible at all times, even if some nodes are offline. Pinata also simplifies the management of "hashes" for stored files, making it easy to check file integrity.

4.3 Front-end application

Next.js [28] is a powerful framework for front-end application development, based on React. It enables the creation of dynamic, responsive and SEO-optimized web applications. In this project, Next.js is used to develop the user interface for our proposed solution, offering users a fluid, interactive experience. Thanks to its server-side rendering capabilities, Next.js ensures fast loading times and smooth transitions, even for complex applications. What's more, it integrates easily with MetaMask, used to manage interactions with Ethereum wallets, enabling secure user authentication and transaction signing within the DApp.

The front-end application will provide users with an intuitive, simple, and user-friendly interface to interact with the blockchain and manage medical records. The solution leverages Next.js for building a fast, scalable, and SEO-friendly web interface with responsive real-time blockchain interactions. Next.js's support for both static and dynamic rendering enables seamless user experiences. For the back-end, Anvil is used, allowing the development of Python-powered logic that integrates smoothly with Web3 technologies, ensuring efficient management of blockchain interactions and medical record processing. This combination of Next.js and Anvil provides a powerful and cohesive platform for both the front-end and back-end of the application.

4.4 Ethereum blockchain

The Ethereum public blockchain will serve as the foundation for recording transactions and interacting with smart contracts. Ethereum's decentralized nature ensures the immutability and transparency of medical data while enabling secure access control mechanisms. Smart contracts deployed on Ethereum will handle critical operations, such as patient registration, access permissions, and record updates.

Smart contracts, written in Solidity, will govern the core functionalities of the system. These contracts will include the following features:

Patient Registration: Enabling the creation of patient profiles with unique identifiers.

Access Control: Implementing role-based permissions to allow only authorized entities (e.g., healthcare providers or patients) to access or update records.

Audit Trails: Automatically logging every interaction for transparency and accountability.

5. THE PROPOSED SOLUTION

Our proposed solution focuses on ensuring the immutability and confidentiality of medical records using blockchain technology. By leveraging the decentralized and tamper-proof nature of blockchain, medical records are stored in a secure, distributed ledger where unauthorized modifications are effectively prevented. For example, patient data can be hashed and stored on the blockchain,

ensuring that only authorized parties with the correct decryption keys can access the original information. This approach mitigates risks associated with traditional centralized systems, such as hacking or unauthorized access to sensitive data.

To further safeguard patient information, the system incorporates advanced encryption techniques to protect medical data. Encryption ensures that even if the data is intercepted during transmission or stored on the blockchain, it remains inaccessible without the proper decryption keys. For instance, using asymmetric cryptography, only healthcare providers or patients with valid private keys can access or modify sensitive information. This guarantees compliance with privacy regulations, such as GDPR or HIPAA, while maintaining patient trust.

The blockchain's inherent transparency ensures that all interactions with medical records are traceable. Every action, such as viewing, updating, or sharing a medical record, is logged on the blockchain as a transaction, complete with timestamps and the identity of the actor (pseudonymized where necessary for privacy). For example, a patient can track when their record was accessed and by whom, creating a clear audit trail. This level of traceability not only increases trust but also helps detect and deter unauthorized activities.

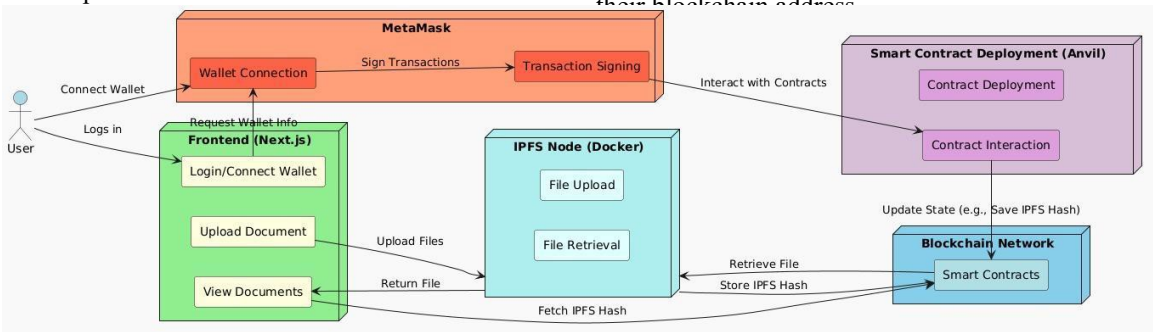

Figure 1: General architecture of the proposed solution

By reducing dependence on a centralized authority, the proposed solution enhances the system's resilience and eliminates single points of failure. In traditional systems, if a central server is compromised or experiences downtime, access to medical records is disrupted. With a decentralized approach, data is distributed across multiple nodes, ensuring continuous availability and protection against cyberattacks. For instance, a patient's medical history would remain accessible even if one or more nodes in the network fail.

Facilitating secure data exchange between various stakeholders is crucial for improving healthcare outcomes. The proposed solution aims to achieve interoperability by adhering to standardized data formats and protocols, enabling seamless sharing of medical records among hospitals, clinics, insurance companies, and patients. For example, a patient treated in one hospital can securely share their medical history with another healthcare provider without the need for manual data transfer. This reduces errors, accelerates diagnosis, and ensures continuity of care.

Regarding patient registration, each one will have a unique address on the blockchain. Basic information about the patient will be securely recorded using a smart contract. This ensures that patient records are uniquely identifiable and tamper-proof.

Healthcare professionals can create and update patients' medical records, which are stored in IPFS. The file hash generated by IPFS is stored on the blockchain, guaranteeing immutability. For example, a new lab report can be added to a patient's record with its hash securely linked to their blockchain address.

Sharing and Accessing Medical Records: Patients have full control over their medical records and can grant or revoke access to specific healthcare providers (hospital, or a doctor for example). Permissions are managed via smart contracts. For instance, a patient can authorize a specialist to view their latest test results for a limited time.

Journal of Theoretical and Applied Information Technology
31st December 2025. Vol.103. No.24

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

To save the audit and history, all actions performed on medical records, such as access, updates, or sharing, are recorded on the blockchain. This provides a complete audit trail, ensuring transparency and enabling patients and providers to trace any modifications or consultations.

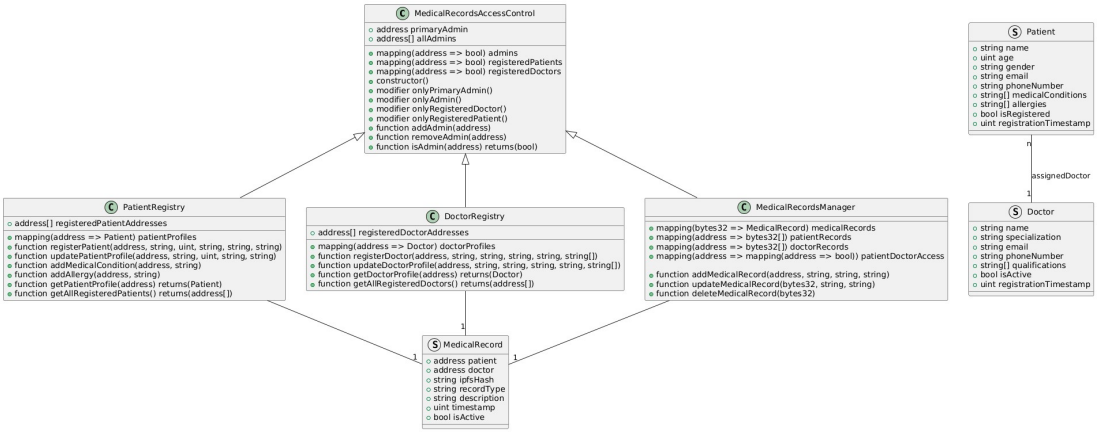

Figure 2: Smart contracts Class Diagram

Sensitive data is encrypted before being uploaded to IPFS, ensuring that even if the data is intercepted or accessed by unauthorized parties, it remains unreadable. Only authorized individuals with the correct decryption keys can access this information, protecting patient privacy.

Decentralized Authentication of users (patients and healthcare providers) is conducted using Ethereum wallets (e.g., MetaMask) or cryptographic private keys. This decentralized approach eliminates the need for traditional username-password systems, reducing the risk of identity theft or unauthorized access.

The architecture, presented in fig. 1, is designed to enable a user to interact with a decentralized system where documents are securely uploaded, stored and accessed. It is based on several interconnected components, each playing an essential role in ensuring that the document management process runs smoothly, from user login to the execution of smart contracts on the blockchain.

The user logs in via the frontend and links his MetaMask wallet to access the system. He can then upload files, manage patients, doctors, admins, etc. depending on the user's role. Documents are stored on IPFS with a hash recorded in a smart contract on the blockchain. To consult a document, it uses the hash to retrieve the file from IPFS. (see fig. 3)

Smart contracts are written and deployed via Remix IDE and tested locally on Ganache and Anvil before being sent to the blockchain using Sepolia test network. They manage hash registration and document information updates.

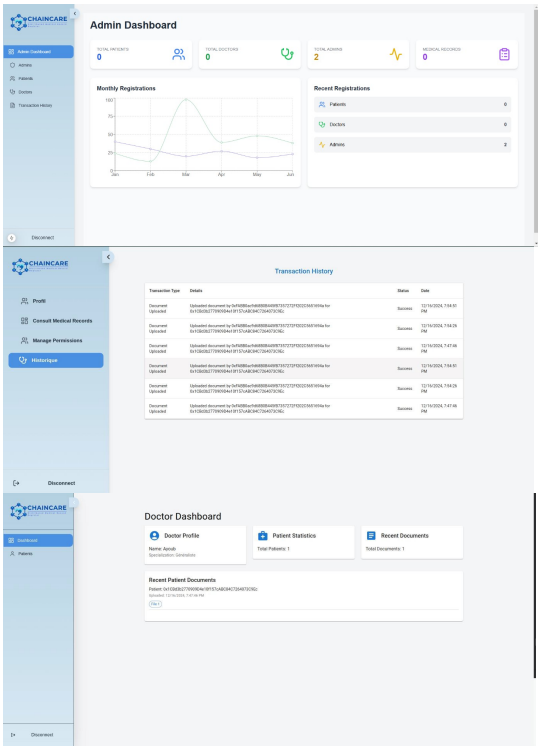

Figure 3: Front end interface: (1) Admin Dashboard (2) Patient history transactions (3) Doctor dashboard

MetaMask enables users to securely sign transactions. Once validated, these transactions are processed by smart contracts on the blockchain, guaranteeing data transparency. IPFS ensures decentralized storage and file integrity. Together, these components enable secure document management.

6. CONCLUSION

In conclusion, this research introduces a groundbreaking approach to addressing the persistent challenges in medical record management through the adoption of blockchain technology. By utilizing Ethereum's decentralized infrastructure, smart contracts, and the InterPlanetary File System (IPFS) for secure and scalable data storage, the proposed system effectively resolves critical issues related to data security, privacy, transparency, and access control. In contrast to conventional centralized systems that are prone to cyberattacks and unauthorized access, this blockchain-based solution ensures immutability, traceability, and decentralization, thereby empowering patients with comprehensive control over their medical information.

The integration of advanced cryptographic techniques, decentralized authentication protocols, and automated workflows powered by smart contracts further enhances the system's robustness and operational efficiency. This innovative framework not only strengthens the reliability and integrity of medical records but also establishes a scalable foundation for future innovations in healthcare data management.

As the healthcare sector increasingly prioritizes decentralized, transparent, and secure solutions, the adoption of blockchain technology marks a transformative step toward building patient-centric, efficient, and trustworthy healthcare ecosystems. This work paves the way for sustained advancements, offering a resilient and forward-looking model for managing sensitive healthcare information in an increasingly digital world.

The perspectives for this project are both extensive and promising, presenting multiple avenues for further advancement and integration within the healthcare sector. One significant area for future development is the scalability of the proposed blockchain-based medical record management system. As the healthcare industry grows and the volume of medical data increases, the solution will need to efficiently manage higher transaction volumes and larger datasets. Future research could explore Layer 2 solutions or alternative blockchain platforms offering higher throughput and lower transaction costs to address these scalability challenges.

Another important direction for future work involves the integration of artificial intelligence (AI) and machine learning (ML) with the blockchain system to enhance decision-making processes and predictive healthcare capabilities. AI algorithms could be applied to analyze patient data stored on the blockchain, thereby providing personalized medical insights while ensuring the data's security and privacy. The combination of AI with decentralized medical records could empower healthcare providers to access actionable insights, ultimately leading to better patient outcomes and more efficient diagnoses.

Interoperability with existing healthcare systems and adherence to global standards represents a crucial consideration for the system's broader adoption. Given that healthcare institutions utilize a variety of software platforms with distinct data structures and privacy protocols, ensuring that the blockchain solution can seamlessly interact with these diverse systems will be essential. Standardizing data formats and communication protocols would enable secure and efficient data exchange among hospitals, clinics, insurance providers, and other stakeholders, without compromising data privacy or integrity.

Additionally, the application of blockchain technology in healthcare could extend beyond medical record management to other areas such as pharmaceutical supply chain management, insurance claims processing, and clinical trial transparency. The integration of blockchain into these domains could contribute to the reduction of fraud, increased transparency, and the optimization of operational workflows throughout the healthcare sector.

Finally, the evolving regulatory landscape presents an important perspective for the success of this system. As blockchain technology disrupts traditional healthcare models, collaboration with regulatory bodies to ensure compliance with data protection laws (such as GDPR and HIPAA) will be essential. By aligning with existing legal frameworks and actively contributing to the development of regulations tailored to decentralized technologies, this solution could play a pivotal role in shaping the future of secure and patient-centered healthcare.

REFERENCES:

[1] P. Bischoff, "Medical Breaches: The undiagnosed cost to millions: A Study," Comparitech. Accessed: Jan. 28, 2025. [Online]. Available: https://www.comparitech.com/blog/vpn-privacy/medical-data-breaches/

[2] S. Alder, "IBM: Average Cost of a Healthcare Data Breach Increases to Almost $11 Million," The HIPAA Journal. Accessed: Jan. 28, 2025. [Online]. Available: https://www.hipaajournal.com/2023-cost-healthcare-data-breach/

[3] A. H. Seh et al., "Healthcare Data Breaches: Insights and Implications," Healthcare, vol. 8, no. 2, Art. no. 2, Jun. 2020, doi: 10.3390/healthcare8020133.

[4] L. H. Newman, "The Worst Hacks of 2024," Wired. Accessed: Jan. 28, 2025. [Online]. Available: https://www.wired.com/story/worst-hacks-2024/

[5] S. Bradley, "Tally of victims reaches 100,000 in NHS cyber-attack." Accessed: Jan. 28, 2025. [Online]. Available: https://www.thetimes.com/uk/scotland/article/tally-of-victims-reaches-100000-in-nhs-cyber-attack-xlsw975cc

[6] A. Minnaar and F. J. Herbig, "Cyberattacks and the Cybercrime Threat of Ransomware to Hospitals and Healthcare Services During the COVID-19 Pandemic," Acta Criminol. Afr. J. Criminol. Vict., vol. 34, no. 3, pp. 155–185, Dec. 2021, doi: 10.10520/ejc-crim_v34_n3_a10.

[7] C. C. McGlave, S. S. Nikpay, C. Henning-Smith, K. Rydberg, and H. T. Neprash, "Characteristics of short-term acute care hospitals that experienced a ransomware attack from 2016 to 2021," Health Aff. Sch., vol. 1, no. 3, p. qxad037, Sep. 2023, doi: 10.1093/haschl/qxad037.

[8] "UCLA Cyber Attack Claimed By CLoP Ransomware Group." Accessed: Jan. 28, 2025. [Online]. Available: https://thecyberexpress.com/ucla-cyber-attack-by-clop-ransomware-group/

[9] K. Chimmanee and S. Jantavongso, "Digital forensic of Maze ransomware: A case of electricity distributor enterprise in ASEAN," Expert Syst. Appl., vol. 249, p. 123652, Sep. 2024, doi: 10.1016/j.eswa.2024.123652.

[10] "Maze ransomware attack will cost Cognizant at least $50m to $70m | Computer Weekly," ComputerWeekly.com. Accessed: Jan. 28, 2025. [Online]. Available: https://www.computerweekly.com/news/252482950/Maze-ransomware-attack-will-cost-Cognizant-at-least-50m-to-70m

[11] Z. Baig, S. H. Mekala, and S. Zeadally, "Ransomware Attacks of the COVID-19 Pandemic: Novel Strains, Victims, and Threat Actors," IT Prof., vol. 25, no. 5, pp. 37–44, Sep. 2023, doi: 10.1109/MITP.2023.3297085.

[12] Wedia, "Millions affected by Dutch data breach: Here's what we know so far," IamExpat. Accessed: Jan. 28, 2025. [Online]. Available: https://www.iamexpat.nl/expat-info/dutch-expat-news/millions-affected-dutch-data-breach-heres-what-we-know-so-far

[13] S. Alder, "The Ransomware Groups Targeting Healthcare Organizations," The HIPAA Journal. Accessed: Jan. 28, 2025. [Online]. Available: https://www.hipaajournal.com/ransomware-groups-targeting-healthcare-organizations/

[14] Evolving Ransomware Attacks on Healthcare Providers - ProQuest. Accessed: Jan. 28, 2025. [Online]. Available: https://www.proquest.com/openview/ded3660de2450a09cfaa6923af000b07/1?pq-origsite=gscholar&cbl=51922&diss=y

[15] M. Alawida, A. E. Omolara, O. I. Abiodun, and M. Al-Rajab, "A deeper look into cybersecurity issues in the wake of Covid-19: A survey," J. King Saud Univ. - Comput. Inf. Sci., vol. 34, no. 10, Part A, pp. 8176–8206, Nov. 2022, doi: 10.1016/j.jksuci.2022.08.003.

[16] A. Shostack and J. Dykstra, "Handling Pandemic-Scale Cyber Threats: Lessons from COVID-19," in Proceedings of the New Security Paradigms Workshop, Sep. 2024, pp. 1–10. doi: 10.1145/3703465.3703466.

[17] T. Emad Ali, F. Imad Ali, M. A. Abdala, A. H. Morad, G. Gódor, and D. Z. Alwahab, "Blockchain-Based Deep Reinforcement Learning System for Optimizing Healthcare," Infocommunications J., vol. 16, no. 3, pp. 89–100, 2024, doi: 10.36244/ICJ.2024.3.9.

[18] R. Sibanda, B. Mutunhu Ndlovu, S. Dube, and K. Maguraushe, Towards Health 4.0: Blockchain-Based Electronic Health Record for Care Coordination, vol. 19. 2024. doi: 10.34190/ecie.19.1.2606.

[19] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," in 2016 2nd International Conference on Open and Big Data (OBD), Aug. 2016, pp. 25–30. doi: 10.1109/OBD.2016.11.

[20] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain," IEEE Access, vol. 5, pp. 14757–14767, 2017, doi: 10.1109/ACCESS.2017.2730843.

[21] "HealthChain: transforming European healthcare through digital solutions and interregional cooperation - European Commission." Accessed: Jan. 28, 2025. [Online]. Available: https://eismea.ec.europa.eu/projects/healthchain-transforming-european-healthcare-through-digital-solutions-and-interregional-cooperation_en

[22] F. Williams and S. Boren, "The role of the electronic medical record (EMR) in care delivery development in developing countries: A systematic review," Inform. Prim. Care, vol. 16, pp. 139–45, Feb. 2008, doi: 10.14236/jhi.v16i2.685.

[23] K. Kaneko, D. Onozuka, H. Shibuta, and A. Hagihara, "Impact of electronic medical records (EMRs) on hospital productivity in Japan," Int. J. Med. Inf., vol. 118, pp. 36–43, Oct. 2018, doi: 10.1016/j.ijmedinf.2018.07.008.

[24] J. Zhang, "A Review of Research on Hospital Electronic Medical Record Management System Based on Cloud Computing," Sci. Technol. Eng. Chem. Environ. Prot., vol. 1, no. 7, Art. no. 7, Jun. 2024, doi: 10.61173/97abz755.

[25] A. Alhur, "Overcoming Electronic Medical Records Adoption Challenges in Saudi Arabia," Cureus, vol. 16, no. 2, p. e53827, doi: 10.7759/cureus.53827.

[26] R. Sandhane, K. Patil, and A. R. Sharma, "Cyber Security Risk Assessment for Electronic Medical Records (EMRs)," in 2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM), Feb. 2024, pp. 1–6. doi: 10.1109/ICIPTM59628.2024.10563486.

[27] "IPFS Documentation | IPFS Docs." Accessed: Jan. 28, 2025. [Online]. Available: https://docs.ipfs.tech/

[28] "Next.js by Vercel - The React Framework." Accessed: Jan. 28, 2025. [Online]. Available: https://nextjs.org/