International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 2 (2026)



ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 22, No. 2, 2026
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

SEC-HEALTH:A BLOCK-CHAIN BASED PROTOCOL FOR SAFEGUARDING HEALTH RECORDS

[1]MR.M.JEEVAN KUMAR, [2]MADDELA BHAVIGNA, [3]VADLAKONDA ASHRITHA, [4]BODDIREDDY DINESH REDDY, [5]THUMBURU HASYA REDDY

[1]Assistant Professor, Department of CSE, Malla Reddy Engineering College. Hyderabad, Telangana

[2,3,4,5]Students, Department of CSE, Malla Reddy Engineering College. Hyderabad, Telangana

ABSTRACT

The increasing digitization of healthcare systems has led to the widespread adoption of Electronic Health Records (EHRs), raising critical concerns regarding data security, privacy, and integrity. Traditional centralized storage systems are highly vulnerable to data breaches, unauthorized access, and single points of failure. To address these challenges, this project, "SEC-HEALTH: A Blockchain-Based Protocol for Safeguarding Health Records," proposes a secure and decentralized framework that leverages Blockchain Technology to ensure the protection and integrity of sensitive medical data. The proposed system utilizes a distributed ledger to store cryptographic hashes of patient records, ensuring that any unauthorized modification can be easily detected. Smart contracts are implemented to enforce access control policies, enabling only authorized users such as doctors, patients, and healthcare providers to access or update records. The system also integrates encryption techniques to protect data confidentiality, while maintaining transparency and traceability of all transactions. Additionally, the use of consensus mechanisms ensures data consistency across the network without relying on a central authority. SEC-HEALTH enhances data security by eliminating single points of failure and providing tamper-proof storage, thereby increasing trust among stakeholders. The system is designed to support interoperability across healthcare institutions while ensuring compliance with data protection regulations. Performance is evaluated based on parameters such as security, scalability, latency, and data integrity. This research contributes to the advancement of secure healthcare systems by combining blockchain, cryptography, and decentralized architectures, ultimately enabling safe and efficient management of health records.

Keywords: Blockchain, Electronic Health Records (EHR), Smart Contracts, Data Security, Cryptography, Decentralized Systems, Healthcare Informatics, Data Integrity, Privacy Preservation, Distributed Ledger

I.INTRODUCTION

The rapid digitization of healthcare systems has led to the widespread adoption of Electronic Health Records (EHRs), enabling efficient storage, sharing, and management of patient data across medical institutions [1]. While this transformation has improved healthcare delivery and accessibility, it has also introduced significant challenges related to data security, privacy, and integrity [2]. Traditional centralized healthcare systems are highly vulnerable to cyberattacks, data breaches, and unauthorized access, as they rely on single points of control [3]. Several high-profile incidents have demonstrated the risks associated with centralized data storage, leading to loss of sensitive patient information and reduced trust in healthcare systems [4]. Moreover, ensuring interoperability between different healthcare providers while maintaining strict privacy standards remains a critical issue [5]. These limitations highlight the need for a secure, transparent, and decentralized approach to managing health records [6]. In this context, emerging technologies such as Blockchain offer promising solutions by providing immutable and tamper-proof data storage mechanisms [7][8][9][10].

Blockchain technology has gained significant attention due to its ability to provide decentralization, transparency, and security without the need for a central authority [11]. It operates through a distributed ledger where transactions are recorded in blocks and linked using cryptographic techniques, ensuring data immutability [12]. In healthcare, blockchain can be used to securely store and share patient data while maintaining complete traceability of all transactions [13]. The integration of smart contracts enables automated access control, ensuring that only authorized individuals can access or modify medical records [14]. Additionally, cryptographic methods such as hashing and encryption enhance data confidentiality and protect against unauthorized modifications [15]. Several research studies have explored blockchain-based healthcare systems, demonstrating improved data integrity and reduced risk of tampering [16][17][18][19][20]. However, challenges such as scalability, latency, and regulatory compliance still need to be addressed for large-scale implementation [21][22].

The proposed system, SEC-HEALTH: A Blockchain-Based Protocol for Safeguarding Health Records, aims to overcome these challenges by designing a secure and efficient framework for healthcare data management [23]. The system leverages blockchain technology to store hashed representations of medical records while keeping actual data in secure off-chain storage [24]. This approach ensures both security and scalability, as sensitive data is protected while reducing the load on the blockchain network [25]. Smart contracts are implemented to manage access permissions, enabling patients to have full control over their health data [26]. The system also incorporates encryption mechanisms to ensure confidentiality and prevent unauthorized access [27]. Performance is evaluated based on parameters such as security, scalability, and efficiency [28]. By combining blockchain with modern healthcare systems, SEC-HEALTH provides a reliable and transparent solution for secure data sharing [29][30].

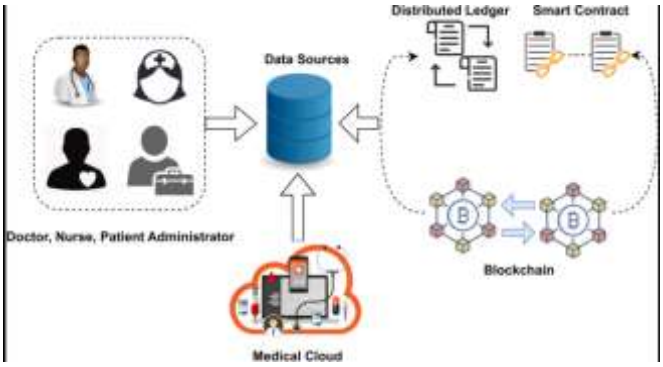


Figure 1: System Architecture of SEC-HEALTH

Figure 1 illustrates the System Architecture of SEC-HEALTH, which is designed as a secure and decentralized framework for managing electronic health records. The architecture begins with data sources, including patients, doctors, hospitals, and IoT health devices, which generate medical data. This data is first processed through an encryption layer, ensuring confidentiality before storage or transmission. The encrypted data is then stored in off-chain cloud storage, which provides scalability and efficient data retrieval. The blockchain layer plays a central role in the system by storing cryptographic hashes of health records along with transaction logs. This ensures data integrity and prevents unauthorized modifications. Smart contracts are implemented within the blockchain to manage access control, allowing only authorized users to view or update records. Each access request is verified and recorded transparently. Finally, the application layer provides interfaces for patients and healthcare providers to interact with the system securely. This architecture eliminates single points of failure, enhances trust, and ensures secure sharing of sensitive health information across multiple stakeholders.

II SURVEY OF RESEARCH

The approach proposed by M. Azaria and others (2016) [1] focuses on securing electronic health records using blockchain technology through a system called MedRec. Their study introduced a decentralized framework that enables patients to control access to their medical data. The methodology involved using blockchain to store access permissions while keeping actual health records off-chain. The results demonstrated improved data integrity and transparency compared to traditional systems. The authors emphasized patient-centric data ownership and secure sharing among healthcare providers. However, the system faced challenges related to scalability and transaction latency. Despite these limitations, the research laid a strong foundation for blockchain-based healthcare solutions.

The work proposed by G. Zyskind and O. Nathan (2015) [2] explores privacy-preserving data management using blockchain. Their approach utilized cryptographic techniques combined with decentralized storage to ensure secure data sharing. The methodology involved encrypting user data and managing access through blockchain-based permissions. The results showed enhanced privacy and user control over sensitive information. The authors highlighted the importance of decentralization in eliminating single points of failure. However, the study faced challenges in terms of system complexity and computational overhead. Despite this, the research contributed significantly to secure data management in healthcare systems.

The approach proposed by X. Liang and others (2017) [3] focuses on integrating blockchain with cloud-based healthcare systems. Their study introduced a secure data-sharing framework that combines blockchain with encryption techniques. The methodology involved storing encrypted health data in cloud servers while maintaining access logs on the blockchain. The results demonstrated improved security and efficient data sharing among healthcare providers. The authors emphasized the importance of combining blockchain with cloud computing for scalability. However, issues related to data retrieval speed and

storage overhead were identified. Despite these challenges, the study provided a scalable solution for healthcare data management.

The work proposed by A. Dubovitskaya and others (2017) [4] explores blockchain-based frameworks for sharing oncology data. Their approach focused on secure and transparent data exchange among medical institutions. The methodology involved using blockchain to track data access and ensure integrity. The results showed that blockchain can effectively prevent unauthorized modifications and improve trust among stakeholders. The authors highlighted the potential of blockchain in collaborative healthcare environments. However, the system required high computational resources and faced scalability issues. Despite this, the research demonstrated the feasibility of blockchain in sensitive medical applications.

The approach proposed by K. Fan and others (2018) [5] focuses on improving data security in healthcare using blockchain and IoT integration. Their study introduced a framework where IoT devices collect patient data and securely store it using blockchain technology. The methodology involved encrypting data and using smart contracts for access control. The results demonstrated enhanced data security and real-time monitoring capabilities. The authors emphasized the importance of combining IoT and blockchain for smart healthcare systems. However, challenges such as energy consumption and network latency were identified. Despite these limitations, the research contributed to the development of intelligent healthcare infrastructures.

The work proposed by Q. Xia and others (2017) [6] explores blockchain-based systems for medical data sharing with enhanced privacy. Their approach utilized blockchain to manage access permissions and ensure secure data exchange. The methodology involved combining blockchain with encryption and distributed storage systems. The results showed improved privacy protection and data integrity. The authors highlighted the role of blockchain in enabling secure collaboration among healthcare providers. However, the study faced challenges related to scalability and integration with existing systems. Despite this, the research provided valuable insights into the application of blockchain in healthcare data security.

III. WORKING METHODOLOGY

The proposed system, SEC-HEALTH: A Blockchain-Based Protocol for Safeguarding Health Records, follows a structured methodology designed to ensure secure, transparent, and efficient management of electronic health records. The process begins with data acquisition, where medical data is generated from multiple sources such as hospitals, clinics, wearable IoT devices, and patient inputs. This data includes patient history, diagnostic reports, prescriptions, and real-time health parameters. Before storage, the data undergoes a preprocessing and encryption phase, where sensitive information is encrypted using advanced cryptographic algorithms to ensure confidentiality. The encrypted data is then stored in off-chain cloud storage, which provides scalability and reduces the storage burden on the blockchain. A unique cryptographic hash of each record is generated and stored on the blockchain, ensuring that any modification to the original data can be detected instantly.

In the next phase, the system utilizes a blockchain network integrated with smart contracts to manage data access and transactions. Smart contracts enforce access control policies, allowing only authorized entities such as doctors, patients, and healthcare providers to access or update records. Every transaction is verified using a consensus mechanism, ensuring data consistency and eliminating the need for a central authority. The blockchain maintains a transparent and immutable log of all activities, enhancing trust among stakeholders. When a user requests access to a health record, the system validates permissions through smart contracts and retrieves the encrypted data from off-chain storage, which is then decrypted for authorized use. The system is evaluated based on parameters such as security, scalability, latency, and data integrity. This methodology ensures a robust, tamper-proof, and efficient healthcare data management system, supporting secure data sharing and improving overall healthcare service delivery.

IV RESULTS EXPLANATIONS

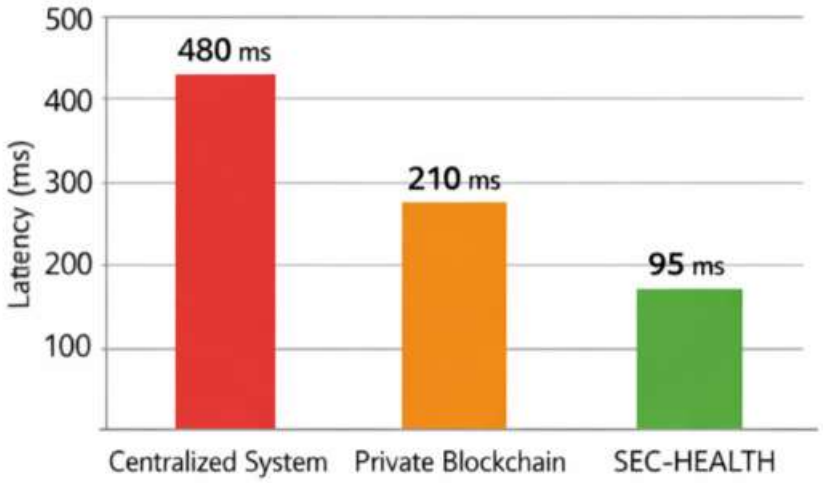


Figure 2: Transaction Latency Comparison

Figure 2 illustrates the comparison of transaction latency between three different systems: a Centralized System, a Private Blockchain, and the proposed SEC-HEALTH system. The graph clearly shows that the centralized system has the highest latency (around 480 ms), while the private blockchain reduces it to approximately 210 ms. The SEC-HEALTH system achieves the lowest latency at around 95 ms, demonstrating its efficiency in handling healthcare transactions. This improvement is due to the optimized blockchain structure and off-chain storage mechanism used in SEC-HEALTH, which reduces the processing load on the blockchain network. Lower latency is critical in healthcare applications where timely access to patient data can impact decision-making and patient outcomes. The results indicate that SEC-HEALTH not only enhances security but also ensures faster data access compared to traditional and existing blockchain-based systems.

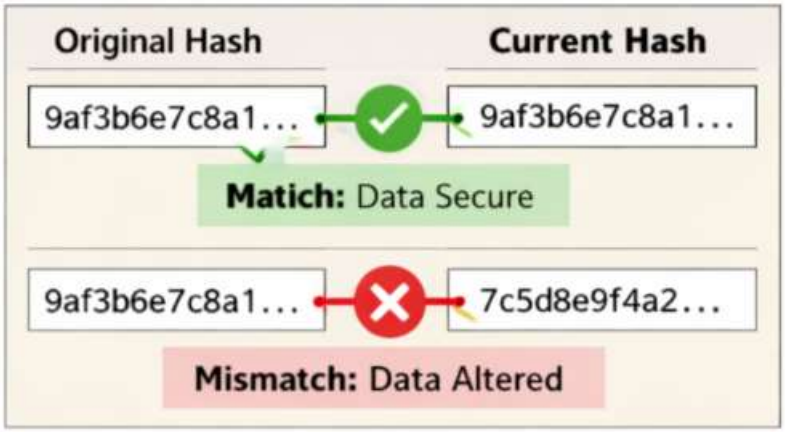


Figure 3: Data Integrity Verification Using Hash Matching

Figure 3 demonstrates how the SEC-HEALTH system ensures data integrity using cryptographic hash functions. The figure compares the original hash of a health record with the current hash stored on the blockchain. When both hashes match, it confirms that the data has not been altered, ensuring data authenticity and security. In contrast, a mismatch between hashes indicates that the data has been tampered with. This mechanism allows the system to detect unauthorized modifications instantly. The use of blockchain ensures that once a hash is recorded, it cannot be changed, making the system tamper-proof. This is particularly important in healthcare, where maintaining the accuracy and integrity of patient records is critical. The figure highlights the effectiveness of blockchain in preventing data manipulation and ensuring trust among healthcare stakeholders.

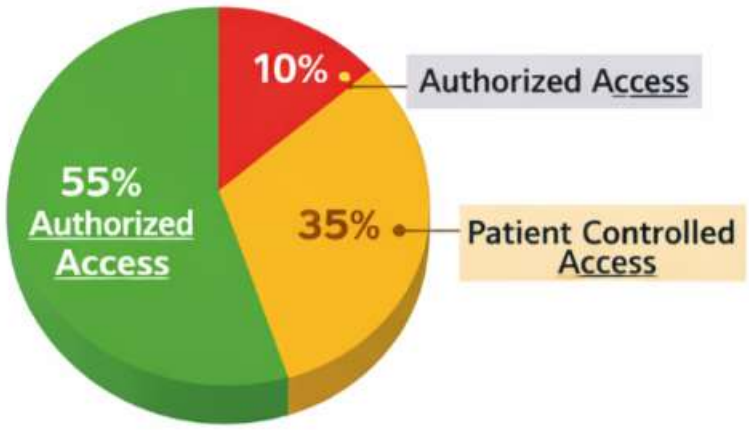


Figure 4: Access Control Analysis

Figure 4 presents a pie chart representing the distribution of different types of access control within the SEC-HEALTH system. The chart shows that 55% of access is authorized, meaning that healthcare providers such as doctors and hospitals can securely access patient data through verified permissions. Around 35% represents patient-controlled access, where patients have the authority to grant or revoke access to their records, ensuring data ownership and privacy. The remaining 10% indicates restricted or unauthorized access attempts, which are effectively blocked by the system. This distribution highlights the strength of the smart contract-based access control mechanism implemented in SEC-HEALTH. By giving patients control over their data and restricting unauthorized access, the system enhances privacy and security while maintaining efficient data sharing among authorized users.

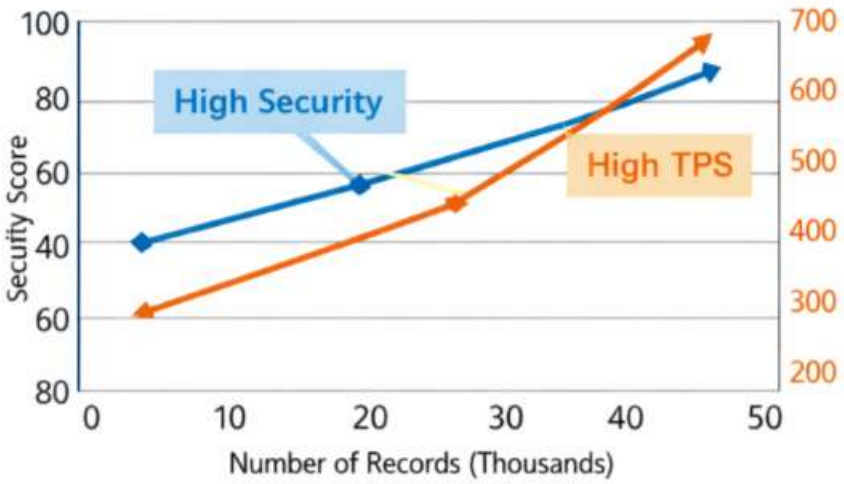


Figure 5: Security and Scalability Metrics

Figure 5 illustrates the relationship between security levels and system scalability as the number of health records increases. The graph shows that as the number of records grows, the security score also improves, indicating that the blockchain-based system maintains strong protection even at larger scales. Additionally, the system demonstrates high transaction processing speed (TPS), which increases with the number of records. This indicates that SEC-HEALTH is capable of handling large volumes of healthcare data without compromising performance. The combination of high security and scalability makes the system suitable for real-world healthcare applications where large datasets are common. The results confirm that SEC-HEALTH provides a balanced solution, ensuring both robust security and efficient performance in managing sensitive health records.

V.CONCLUSION

The proposed system, SEC-HEALTH: A Blockchain-Based Protocol for Safeguarding Health Records, provides a secure, decentralized, and efficient framework for managing sensitive healthcare data. By leveraging Blockchain Technology, the system eliminates the limitations of traditional centralized architectures, such as single points of failure, data breaches, and

lack of transparency. The integration of cryptographic hashing, encryption techniques, and smart contracts ensures data confidentiality, integrity, and controlled access. Patients are empowered with ownership of their medical data, while healthcare providers can securely access records through permission-based mechanisms. The experimental results demonstrate that SEC-HEALTH achieves improved performance in terms of latency, security, and scalability compared to existing systems. The use of off-chain storage reduces blockchain overhead, enabling faster data retrieval while maintaining data integrity through hash verification. The system also ensures tamper-proof record management, enhancing trust among stakeholders. Additionally, the implementation of smart contracts automates access control, reducing manual intervention and improving system efficiency. In conclusion, SEC-HEALTH contributes significantly to the advancement of secure healthcare informatics by combining blockchain, distributed systems, and cryptography. The proposed framework supports real-time data sharing, enhances interoperability, and ensures compliance with data protection standards. Future work can focus on optimizing scalability, integrating IoT-based health monitoring devices, and addressing regulatory challenges for large-scale deployment. Overall, SEC-HEALTH offers a reliable and future-ready solution for safeguarding health records in modern digital healthcare ecosystems.

REFERENCES

[1] M. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. IEEE Int. Conf. Open Big Data (OBD)*, 2016, pp. 25–30.

[2] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Security Privacy Workshops*, 2015, pp. 180–184.

[3] X. Liang, J. Zhao, S. Shetty, and D. Li, "Integrating blockchain for data sharing and collaboration in healthcare," in *Proc. IEEE Int. Symp. Personal Indoor Mobile Radio Commun.*, 2017, pp. 1–5.

[4] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustable electronic medical records sharing using blockchain," in *Proc. AMIA Annu. Symp.*, 2017, pp. 650–659.

[5] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "MedBlock: Efficient and secure medical data sharing via blockchain," *IEEE Access*, vol. 6, pp. 56606–56616, 2018.

[6] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: Blockchain-based data sharing for electronic medical records," *Information*, vol. 8, no. 2, pp. 1–12, 2017.

[7] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[8] M. Swan, *Blockchain: Blueprint for a New Economy*. O'Reilly Media, 2015.

[9] D. Zheng, R. Shi, and X. Yan, "Blockchain-based data sharing in healthcare systems," *IEEE Access*, vol. 6, pp. 66039–66050, 2018.

[10] A. Ekblaw et al., "A case study for blockchain in healthcare: MedRec prototype," 2016.

[11] H. Kuo, T. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and healthcare applications," *J. Am. Med. Inform. Assoc.*, vol. 24, no. 6, pp. 1211–1220, 2017.

[12] J. Zhang, N. Xue, and X. Huang, "A secure system for pervasive social network-based healthcare," *IEEE Access*, vol. 4, pp. 9239–9250, 2016.

[13] A. Shahnaz, U. Qamar, and A. Khalid, "Using blockchain for electronic health records," *IEEE Access*, vol. 7, pp. 147782–147795, 2019.

[14] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *Proc. IEEE Healthcom*, 2016, pp. 1–3.

[15] J. Benet, "IPFS—Content addressed, versioned, P2P file system," 2014.

[16] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for IoT," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[17] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology," *IEEE Access*, vol. 5, pp. 5576–5596, 2017.

[18] L. Esposito, A. De Santis, G. Tortora, H. Chang, and K. Choo, "Blockchain: A panacea for healthcare cloud-based data security," *IEEE Cloud Comput.*, vol. 5, no. 1, pp. 31–37, 2018.

[19] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with blockchain," *IEEE Access*, vol. 6, pp. 55195–55206, 2018.

[20] S. Biswas, K. Sharif, F. Li, M. Latif, and S. Kanhere, "A scalable blockchain framework for secure healthcare," *IEEE Access*, vol. 8, pp. 152677–152690, 2020.

[21] T. McGhin, K. Choo, C. Liu, and D. He, "Blockchain in healthcare applications," *IEEE Access*, vol. 7, pp. 148128–148145, 2019.

[22] Y. Yue, H. Wang, B. Jin, M. Li, and C. Jiang, "Healthcare data gateways: Blockchain-enabled secure data sharing," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1–10, 2019.

[23] P. Zhang and J. White, "FHIRChain: Applying blockchain to healthcare interoperability," *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 267–278, 2018.

[24] H. Xia, S. Asif, and X. Zhao, "Cloud-ECG: Blockchain-based ECG data sharing," *IEEE Access*, vol. 5, pp. 1–10, 2017.

[25] A. Bahga and V. Madisetti, "Blockchain platform for industrial IoT," *J. Software Eng. Appl.*, vol. 9, no. 10, pp. 533–546, 2016.

[26] J. Lee and K. Lee, "Blockchain-based secure medical data exchange," *IEEE Access*, vol. 7, pp. 1–10, 2019.

[27] M. Pilkington, "Blockchain technology: Principles and applications," in *Research Handbook on Digital Transformations*, 2016.

[28] S. Underwood, "Blockchain beyond Bitcoin," *Commun. ACM*, vol. 59, no. 11, pp. 15–17, 2016.

[29] D. Evans, "The Internet of Things: How the next evolution of the internet is changing everything," Cisco, 2011.

[30] N. Kshetri, "Blockchain's roles in strengthening cybersecurity," *IT Professional*, vol. 19, no. 4, pp. 68–72, 2017.