International Journal of Engineering Trends and Applications (IJETA) – Volume 12 Issue 5, Sep-Oct 2025

RESEARCH ARTICLE OPEN ACCESS

Blockchain and Cybersecurity: A Comprehensive Review

Aditi Biswas*

*(School of Computer Applications, JECRC University, Jaipur, Rajasthan, India)

ABSTRACT

The growing number and complexity of cyber threats have created a strong need for more reliable and secure digital solutions. Traditional cybersecurity methods, while useful, often face problems like single points of failure, data leaks, and lack of trust or transparency. Blockchain technology is now being seen as a promising solution because of its decentralized design, immutability, transparency, and secure validation process. This review paper explores how blockchain can improve cybersecurity by discussing its main features and working principles. Key applications include secure data sharing, identity management, intrusion detection, supply chain security, and protection against Distributed Denial of Service (DDoS) attacks. The paper also outlines the major challenges in adopting blockchain, such as scalability issues, high energy use, interoperability, and regulatory barriers. Finally, it highlights future opportunities, especially when blockchain is combined with technologies like artificial intelligence (AI), machine learning (ML), and the Internet of Things (IoT), to build advanced and adaptive security systems. Overall, this study shows that blockchain has great potential to transform cybersecurity, but further research and development are needed to overcome its challenges and unlock its full benefits.

Keywords —Cybersecurity, Blockchain, Malware attack, Cybercriminals.

1. INTRODUCTION

The rapid advancement of digital technologies has transformed various sectors, enabling seamless communication, online transactions, and data sharing. However, this progress has also led to a significant rise in cyber threats, including data breaches, identity theft, malware attacks, and ransomware. Cybercriminals continuously develop sophisticated techniques to exploit vulnerabilities in traditional security systems, making it increasingly difficult for organizations and individuals to safeguard sensitive data.

Conventional cybersecurity measures, such as firewalls, antivirus software, and centralized authentication systems, often struggle to keep pace with the evolving threat landscape. These systems typically rely on centralized servers, which can become single points of failure, making them prime targets for hackers. Additionally, data stored on centralized platforms is more susceptible to unauthorized access and manipulation.

Blockchain technology has emerged as a promising solution to address these cybersecurity challenges. As a decentralized and distributed ledger system, blockchain enhances security by ensuring data integrity, transparency, and resistance to tampering. Each transaction recorded on a blockchain is encrypted and linked to the previous transaction, making it nearly impossible for attackers to alter information without detection. Furthermore, its consensus mechanisms, such as Proof of Work (PoW) and Proof of Stake (PoS), add an additional layer of security by validating transactions in a trustless environment.

By integrating blockchain technology into cybersecurity frameworks, organizations can enhance authentication processes, prevent fraud, and protect sensitive data from cyber threats. This paper explores the role of blockchain in cybersecurity, its key applications, potential challenges, and future prospects in securing digital ecosystems.

2. KEY FEATURES OF BLOCKCHAIN IN CYBERSECURITY

Blockchain technology offers several key advantages that enhance cybersecurity by providing a secure, transparent, and tamper-resistant framework for data protection. These

advantages help mitigate cyber threats and improve overall security measures in digital ecosystems.

Decentralization: Traditional cybersecurity models rely on centralized servers, making them vulnerable to cyberattacks, data breaches, and system failures. Blockchain operates on a decentralized network, where data is distributed across multiple nodes. This eliminates single points of failure, reducing the risk of hacking attempts and unauthorized access. Even if one node is compromised, the rest of the network remains unaffected, ensuring greater resilience against cyber threats.

Immutability: One of the most significant features of blockchain is its immutability. Once a transaction is recorded on the blockchain, it cannot be altered, deleted, or tampered with. This ensures data integrity and prevents malicious actors from modifying information. The use of cryptographic hashing further strengthens security by creating a verifiable and irreversible record of all transactions, making blockchain an ideal solution for protecting sensitive data.

Cryptographic Security: Blockchain employs advanced cryptographic techniques to secure transactions and data storage. Public-key cryptography (PKC), digital signatures, and hashing algorithms ensure that only authorized parties can access and verify data. These encryption mechanisms make it extremely difficult for hackers to manipulate or steal information, significantly enhancing cybersecurity.

Transparency and Trust: Blockchain maintains a transparent and publicly verifiable ledger of transactions. Each transaction is recorded with a timestamp and linked to previous entries, providing a clear audit trail. This transparency increases accountability and trust among users, making it easier to detect fraud, unauthorized changes, or malicious activities. Organizations can leverage this feature to enhance data security and compliance with regulatory standards.

Smart Contracts: Smart contracts are self-executing contracts with predefined rules and conditions embedded within the blockchain. These digital agreements automate security policies and execute transactions without human intervention, reducing the risk of fraud and errors. Smart contracts enhance cybersecurity by enforcing access control, verifying identities, and ensuring that only authorized actions are performed within a system.

By integrating blockchain technology into cybersecurity frameworks, organizations can strengthen data protection, reduce cyber threats, and establish a more secure digital environment. However, while blockchain offers numerous advantages, challenges such as scalability, energy consumption, and regulatory concerns must also be addressed for widespread adoption.

3. APPLICATIONS OF BLOCKCHAIN IN CYBERSECURITY

To Blockchain technology is being widely adopted across various industries to enhance cybersecurity by providing secure, transparent, and tamper-proof solutions. Its decentralized and cryptographic nature ensures data integrity, prevents unauthorized access, and protects digital assets from cyber threats. Below are some key areas where blockchain is improving cybersecurity:

Identity Management: Identity theft and unauthorized access are major cybersecurity concerns. Traditional identity management systems rely on centralized databases, which are vulnerable to hacking and data breaches. Blockchain-based identity management systems provide a decentralized and secure way of storing and verifying digital identities. Users have full control over their personal data, reducing the risk of identity fraud. With blockchain, organizations can implement secure authentication mechanisms, such as self-sovereign identities (SSI), where individuals verify their credentials without relying on third-party authentication services.

Secure Data Storage: Storing sensitive data on centralized cloud servers increases the risk of cyberattacks, data leaks, and unauthorized modifications. Blockchain-based decentralized storage solutions, such as InterPlanetary File System (IPFS) and Storj, distribute data across multiple nodes, making it more resilient to

breaches. Data is encrypted and stored in a tamper-proof manner, ensuring its security and integrity. Organizations in healthcare, finance, and government sectors are increasingly adopting blockchain for secure data management to protect confidential records from cyber threats.

IoT Security: The Internet of Things (IoT) connects billions of smart devices, but many of these devices lack strong security measures, making them susceptible to cyberattacks. Hackers can exploit vulnerabilities in IoT systems to gain unauthorized access, steal data, or launch large-scale distributed denial-of-service (DDoS) attacks. Blockchain enhances IoT security by creating a decentralized and immutable ledger for device authentication and communication. Each device in the network is assigned a unique identity on the blockchain, ensuring only trusted devices can interact with one another. This prevents unauthorized access and enhances the overall security of IoT ecosystems.

Fraud Prevention: Financial fraud, such as money laundering and payment fraud, is a growing cybersecurity challenge. Blockchain's transparency and immutability make it an effective tool for detecting and preventing fraudulent activities. Every transaction recorded on the blockchain is time-stamped and cannot be altered, providing a clear audit trail for financial institutions. Smart contracts can also be used to automate fraud detection processes by setting predefined rules that trigger alerts when suspicious transactions occur. This technology is widely used in banking, supply chain management, and e-commerce to enhance security and reduce fraud.

Secure Communication: Traditional communication platforms often lack strong encryption, making them vulnerable to eavesdropping, data breaches, and cyber espionage. Blockchain-based encrypted messaging systems ensure privacy and data protection by providing end-to-end encryption. Messages are stored in a decentralized and tamper-proof manner, preventing unauthorized access or interception. Secure communication platforms built on blockchain, such as Whisper and Status, offer enhanced privacy for users by eliminating reliance on central servers. These solutions are particularly beneficial for industries that require confidential communication, such as government agencies, healthcare institutions, and corporate businesses.

By leveraging blockchain technology, organizations can strengthen cybersecurity measures, protect sensitive information, and prevent cyber threats across various domains. While blockchain-based security solutions offer significant advantages, further advancements in scalability, regulatory compliance, and interoperability are needed for widespread adoption.

4. CHALLENGES OF IMPLEMENTING BLOCKCHAIN IN CYBERSECURITY

While blockchain offers significant advantages in enhancing cybersecurity, several challenges limit its widespread adoption. These challenges must be addressed to fully leverage blockchain's potential in securing digital systems. Below are some of the key challenges:

Scalability Issues: Blockchain networks often face scalability problems as transaction volumes increase. Public blockchains, such as Bitcoin and Ethereum, require every transaction to be verified by multiple nodes, leading to slower processing times and higher latency. As more users join the network, the system can become congested, making it difficult to support real-time applications. To address scalability, researchers are exploring solutions such as sharding, layer-2 protocols (e.g., Lightning Network, Plasma), and alternative consensus mechanisms that enhance transaction speeds without compromising security.

High Energy Consumption: Certain blockchain consensus mechanisms, such as Proof-of-Work (PoW), require extensive computational power to validate transactions. The mining process in PoW-based blockchains consumes a significant amount of energy, making it environmentally unsustainable. This high energy consumption poses a challenge for organizations looking to integrate blockchain into cybersecurity without increasing their carbon

footprint. Alternatives like Proof-of-Stake (PoS), Delegated Proof-of-Stake (DPoS), and Proof-of-Authority (PoA) are being explored to provide energy-efficient blockchain solutions while maintaining security and decentralization.

Regulatory and Compliance Concerns: The regulatory landscape for blockchain technology remains uncertain in many regions. Governments and regulatory bodies are still developing frameworks to address concerns related to privacy, data ownership, and legal accountability in blockchain-based security systems. The lack of clear regulations creates uncertainty for businesses and organizations, making it difficult to adopt blockchain for cybersecurity applications. Additionally, compliance with data protection laws, such as the General Data Protection Regulation (GDPR), can be challenging, as blockchain's immutability conflicts with the right to data deletion (right to be forgotten).

Integration Complexity and Costs: Implementing blockchain within existing cybersecurity frameworks can be complex and expensive. Many organizations rely on legacy security systems that are not designed to integrate with decentralized technologies. Transitioning from traditional centralized security models to blockchain-based solutions requires significant investment in infrastructure, software development, and employee training. Furthermore, blockchain networks need to be interoperable with existing IT systems and security tools to ensure seamless integration, which adds another layer of complexity.

Potential Vulnerabilities in Smart Contracts and Private Keys: While blockchain itself is highly secure, vulnerabilities in smart contracts and private key management can be exploited by cybercriminals. Smart contracts are self-executing code stored on the blockchain, and if not properly audited, they can contain bugs or loopholes that attackers can exploit. High-profile security breaches, such as the DAO attack on Ethereum, have demonstrated the risks associated with poorly designed smart contracts. Additionally, private keys are crucial for accessing blockchain-based assets and systems. If a private key is lost or stolen, the associated data or digital assets cannot be recovered, leading to security risks for users and organizations.

5. FUTURE PROSPECTS OF BLOCKCHAIN IN CYBERSECURITY

Blockchain technology is continuously evolving, and its integration with other advanced technologies such as artificial intelligence (AI) and quantum computing holds great potential for enhancing cybersecurity. Future research should focus on:

- Developing energy-efficient consensus mechanisms.
- Enhancing interoperability between blockchain networks.
- Strengthening smart contract security.
- Establishing global regulatory standards for blockchain applications

6. CONCLUSIONS

Blockchain technology is a powerful tool for improving cybersecurity. It offers decentralization, transparency, immutability, and strong encryption to protect data. It is widely used in identity management, secure data storage, IoT security, fraud prevention, and secure communication. However, challenges like scalability, high energy use, regulatory issues, and security risks in smart contracts and private keys limit its adoption. Continuous research and innovation are needed to overcome these issues. The future of blockchain in cybersecurity looks promising, with improvements in energy-efficient processes, better integration with other technologies like AI and quantum computing, and stronger security measures. Collaboration among industry leaders, researchers, and policymakers will help set standards and drive wider adoption. With further development, blockchain can play a key role in building a safer digital world..

REFERENCES

[1] A. Agarwal, R. Joshi, H. Arora and R. Kaushik, "Privacy and Security of Healthcare Data in Cloud based on the Blockchain Technology," 2023 7th

International Conference on Computing Methodologies and Communication (ICCMC), pp. 87-92, 2023.

[2] S. Mishra, H. Arora, G. Parakh and J. Khandelwal, "Contribution of Blockchain in Development of Metaverse," 2022 7th International Conference on Communication and Electronics Systems (ICCES), pp. 845-850, 2022.

[3] A. Agarwal, R. Joshi, H. Arora and R. Kaushik, "Privacy and Security of Healthcare Data in Cloud based on the Blockchain Technology," 2023 7th International Conference on Computing Methodologies and Communication (ICCMC), pp. 87-92, 2023.

[4] H. Arora, T. Manglani, G. Bakshi and S. Choudhary, "Cyber Security Challenges and Trends on Recent Technologies," 2022 6th International Conference on Computing Methodologies and Communication (ICCMC), pp. 115-118, 2022.

[5] Rahul Misra, Dr. Ramkrishan Sahay, "Evaluation of Student Performance Prediction Models with Two Class Using Data Mining Approach", International Journal of Recent Research and Review, Vol. 11, Issue. 1, pp. 71-79, 2018.

[6] G. K. Soni, A. Rawat, S. Jain and S. K. Sharma, "A Pixel-Based Digital Medical Images Protection Using Genetic Algorithm with LSB Watermark Technique", Springer Smart Systems and IoT: Innovations in Computing. Smart Innovation, Systems and Technologies, Vol. 141, pp. 483-492, 2020.

[7] Hemant Sharma Nimay Seth, Harshita Kaushik , Khushboo Sharma, "A comparitive analysis for Genetic Disease Detection Accuracy Through Machine Learning Models on Datasets", International Journal of Enhanced Research in Management & Computer Applications, Vol. 13, Issue. 8, 2024.

[8] H. Kaushik, K. D. Gupta, "Machine learning based framework for semantic clone detection", Recent Advances in Sciences, Engineering, Information Technology & Management, pp. 52-58, 2025.

[9] H. Kaushik, K. D Gupta, "Code Clone Detection: An Empirical Study of Techniques for Software Engineering Practice", Lampyrid: The Journal of Bioluminescent Beetle Research, Vol. 13, pp. 61-72, 2023.

[10] H. Arora, R. Agarwal, P. Sharma, G. Shankar and D. Arora, "Image Security Utilizing Hybrid Model of Steganography and Asymmetric Cryptography Methods," 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), pp. 277-280, 2023.

[11] H. Arora, P. Kumar Sharma, K. Mitanshi and A. Choursia, "Enhanced Security of Digital Picture and Text Information with Hybride Model of Hiding and Encryption Techniques," 2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), pp. 1238-1241, 2022.

[12] Rahul Misra, "A Novel Approach to Enhanced Digital Image Encryption Using the RSA Algorithm", International Conference on Engineering & Design (ICED), 2021.

[13] H. Kaushik, "Artificial Intelligence in Healthcare: A Review", International Journal of Engineering Trends and Applications (IJETA), Vol. 11, Issue. 6, pp. 58-61, 2024.

[14] N. Tiwari, D. Goyal, and N. Hemrajani, “A hybrid method for image watermarking,” International Journal of Advanced Research in Computer Engineering and Technology (IJARCET), vol. 6, no. 6, pp. 894–898, 2017.

[15] G. Sharma, N. Hemrajani, S. Sharma, A. Upadhyay, Y. Bhardwaj, and A. Kumar, “Data management framework for IoT edge-cloud architecture for resource-constrained IoT application,” Journal of Discrete Mathematical Sciences and Cryptography, vol. 25, no. 4, pp. 1093–1103, 2022.

[16] M. Dahiya, N. Hemrajani, A. Kumar, S. Rani, and S. Rathee, Artificial Intelligence in Medicine and Healthcare. Abingdon, U.K.: Taylor & Francis, 2025.

[17] H. Kaushik, "Artificial Intelligence: Recent Advances, Challenges, and Future Directions", International Journal of Engineering Trends and Applications (IJETA), Vol. 12, Issue. 2, 2025.

[18] Rahul Misra, Dr. Ramkrishan Sahay, "A Review on Student Performance Predication Using Data Mining Approach", International Journal of Recent Research and Review, Vol. 10, Issue. 4, pp. 45-47, 2017.

[19] Rahul Misra, Dr. Ramkrishan Sahay, "Evaluation of Five-Class Student Model based on Hybrid Feature Subsets", International Journal of Recent Research and Review, Vol. 11, Issue. 1, pp. 80-86, 2018.

[20] G. K. Soni, H. Arora, B. Jain, "A Novel Image Encryption Technique Using Arnold Transform and Asymmetric RSA Algorithm", Springer International Conference on Artificial Intelligence: Advances and Applications 2019 Algorithm for Intelligence System, pp. 83-90, 2020.

[21] V. Singh, M. Choubisa, G. K. Soni, "Enhanced Image Steganography Technique for Hiding Multiple Images in an Image Using LSB Technique", TEST Engineering Management, vol. 83, pp. 30561-30565, May-June 2020.

[22] H. Arora, G. K. Soni, R. K. Kushwaha and P. Prasoon, "Digital Image Security Based on the Hybrid Model of Image Hiding and Encryption," 2021 6th International Conference on Communication and Electronics Systems (ICCES), pp. 1153-1157, 2021.

[23] S. A. Saiyed, N. Sharma, H. Kaushik, P. Jain, G. K. Soni and R. Joshi, "Transforming portfolio management with AI and ML: shaping investor perceptions and the future of the Indian investment sector," Parul University International Conference on Engineering and Technology 2025 (PiCET 2025), pp. 1108-1114, 2025.

[24] H. Mathur and R. Ajmera, "Enhancing service efficiency and ensuring privacy in distributed computing environments through a MapReduce based framework," Tuijin Jishu/Journal of Propulsion Technology, vol. 44, no. 6, 2023.

[25] H. Kaushik, I. Yadav, R. Yadav, N. Sharma, P. K. Sharma and A. Biswas, "Brain tumor detection and classification using deep learning techniques and MRI imaging," Parul University International Conference on Engineering and Technology 2025 (PiCET 2025), pp. 1453-1457, 2025.

[26] A. Kumar and N. Hemrajani, "Comparative analysis of different transport layer protocol techniques in cognitive network," Recent Advances in Computer Science and Communications, 2024.

[27] A. Kumar and N. Hemrajani, "Congestion avoidance in TCP based on optimized random forest with improved random early detection algorithm," International Journal of Image and Graphics, 2024.

[28] H. Kaushik, H. Arora, R. Joshi, K. Sharma, M. Mehra and P. K. Sharma, "Digital Image Security using Hybrid Model of Steganography and Cryptography," 2025 International Conference on Electronics and Renewable Systems (ICEARS), pp. 1009-1012, 2025.

[29] H. Mathur and R. Ajmera, "Optimizing service efficiency and safeguarding privacy in distributed computing environments via a MapReduce-powered framework," International Development Planning Review, vol. 47, 2023.