IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, January 2026
Impact Factor: 7.67

Blockchain Application in Network Security

Asmita Rajeshwar Salgaonkar[1], Arshiya Minhaj Shaikh[2], Shraddha shrikant Dokhale[3], Prof. N. S. Kharatmal[4]
Student, Computer Science and Engineering [1,2,3]
Lecturer , Computer Science and Engineering[4]
Matsyodari Shikshan Sanstha Collage of Engineering and Polytechnic, Jalna, India
asmitasalgaonkar18@gmail.com, arshmin08@gmail.com,
shraddhadokhale08@gmail.com, nanditakharatmal1126@gmail.com

Abstract: *The increasing dependence on computer networks for communication, data sharing, and online services has significantly raised concerns regarding network security. Modern networks are frequently targeted by various cyber threats, including unauthorized access, data breaches, identity spoofing, man-in-the-middle attacks, and distributed denial-of-service (DDoS) attacks. Traditional network security solutions such as centralized authentication servers, firewalls, and intrusion detection systems often face limitations related to single points of failure, lack of transparency, and trust dependency on third-party authorities. These challenges highlight the need for more robust, decentralized, and trustworthy security mechanisms.Blockchain technology has emerged as a promising solution to address these security challenges due to its decentralized, immutable, and transparent nature.*

This paper presents a comprehensive survey of blockchain applications in network security. It explores how blockchain technology can be effectively utilized to improve key security aspects such as secure authentication, access control, data integrity verification, secure communication, and resistance against common cyber-attacks. The study reviews existing research works in this domain and analyzes different blockchain-based security models proposed by researchers. A comparative analysis between traditional network security approaches and blockchain-based solutions is also provided to highlight the advantages and limitations of each.

Keywords: Blockchain, Network Protection, Cyber Security, Distributed Ladger, Secure Communication

I. INTRODUCTION

The rapid growth of digital systems and networks has created new security challenges, with traditional security measures often falling short in addressing these threats. Network security has become a critical concern, with data breaches and cyber-attacks becoming increasingly sophisticated. According to a recent report, the global cost of cybercrime is projected to reach $10.5 trillion by 2025, highlighting the need for innovative security solutions [1].

Blockchain technology, initially designed for cryptocurrency transactions, has emerged as a promising solution to enhance network security. Its decentralized, immutable, and transparent nature makes it an attractive solution for secure data management. The use of blockchain in network security has been explored in various applications, including secure data sharing, identity management, and threat detection.

II. LITERACY SURVAY

Previous research on blockchain-based network security has mainly focused on improving trust, data integrity, and resistance to cyber-attacks. The major contributions from existing studies are summarized below:

1) Decentralized Security Models: Researchers proposed blockchain-based decentralized security architectures to remove single points of failure present in traditional centralized systems. These models improve transparency and trust among network participants.

2) Authentication and Access Control: Several studies introduced blockchain-enabled authentication mechanisms to securely verify user identities and manage access rights. These approaches reduce dependency on centralized authentication servers and minimize identity-related attacks.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, January 2026 Impact Factor: 7.67

3) Data Integrity and Secure Logging: Blockchain has been widely used to maintain immutable logs of network transactions and communication events. This ensures data integrity and allows easy detection of unauthorized data modification.

4) DDoS Attack Mitigation: Some researchers explored blockchain-based solutions to prevent distributed denial-of-service (DDoS) attacks by validating legitimate nodes before allowing network access. These solutions enhance attack resistance but may face performance challenges.

5) Blockchain in IoT Networks: Studies highlighted the use of blockchain for securing IoT environments by providing secure device authentication and data validation. However, resource constraints and scalability remain major concerns.

Despite these contributions, existing research reveals limitations related to scalability, latency, and real-world implementation. These challenges indicate the need for efficient and lightweight blockchain-based security frameworks. This paper aims to analyze current research, compare existing solutions, and identify future directions for blockchain applications in network security.

III. EXISTING MODEL

The existing network security model is mainly centralized in nature. In this model, security operations such as authentication, authorization, monitoring, and data protection are controlled by a central authority or server**.**.

Key components of the existing model:

Central Authentication Server: User identities are verified using a single centralized server (username, password, certificates).

Firewalls: Used to filter incoming and outgoing network traffic based on predefined rules.

Intrusion Detection/Prevention Systems (IDS/IPS): Monitor network traffic to detect suspicious or malicious activities.

Centralized Log Management: Network logs and records are stored in a central database for monitoring and auditing.

Third-party Trust: The system relies on trusted third parties (servers or administrators) to manage security. Traditional security mechanisms including firewalls, intrusion detection and prevention systems, and centralized authentication servers are commonly used to protect network resources. Cryptographic algorithms such as AES and RSA are applied to secure data transmission, while hashing techniques are used for password protection and integrity verification. Although this model provides basic security, it suffers from several limitations such as single points of failure, lack of transparency, and high dependency on trusted third parties. If the central authority is compromised, the entire network becomes vulnerable to cyber-attacks, data manipulation, and insider threats. These drawbacks highlight the need for more decentralized and trustworthy security solutions.

IV. PURPOSE / WORKING MODEL AND METHODOLOGY

A. Purpose/Working

The purpose of the proposed blockchain-based network security model is to overcome the limitations of traditional centralized security systems by providing a decentralized, transparent, and tamper-resistant security framework. Conventional network security mechanisms depend on a central authority for authentication and access control, which leads to single points of failure and trust issues. In the proposed model, blockchain technology is used to securely manage authentication, access permissions, and security events in a distributed manner. All network users or devices are registered on the blockchain, and every access request is verified through cryptographic techniques and consensus mechanisms. Once verified, the access information and security events are recorded as immutable transactions on the blockchain. This decentralized working approach ensures data integrity, prevents unauthorized modification, eliminates reliance on third-party trust, and enhances resistance against attacks such as identity spoofing, data tampering, and distributed denial-of-service attacks.

B. Methodology

The methodology followed in this research paper is primarily survey-based and analytical. The steps involved are as follows:

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, January 2026
Impact Factor: 7.67

1) Study of Traditional Network Security Models: Analysis of existing centralized security mechanisms and their limitations.

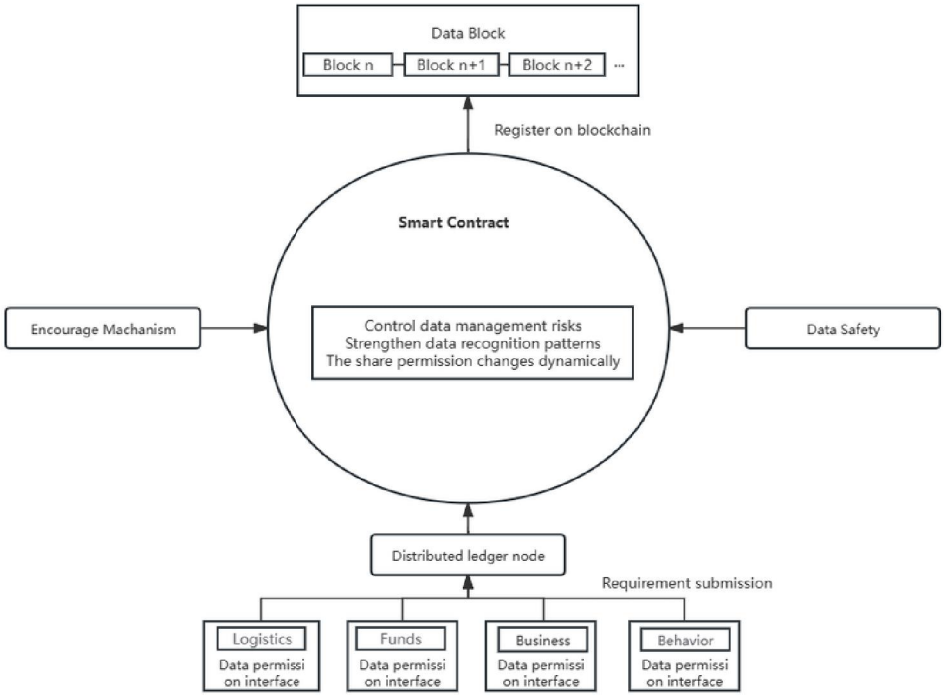
2) Blockchain Technology Analysis: Understanding blockchain features such as decentralization, immutability, cryptographic hashing, and consensus mechanisms.

3) Literature Survey: Review of existing research papers related to blockchain applications in network security.

4) Comparative Analysis: Comparison between traditional security models and blockchain-based security approaches based on parameters such as security, transparency, trust, and scalability.

5) Proposed Conceptual Model: Design of a blockchain-based network security framework to address identified security issues.

6) Result Discussion and Future Scope: Analysis of benefits, challenges, and future improvements including AI and IoT integration.



V. ALGORITHM USED IN EXISTING MODEL

Algorithm Type	Algorithm Used	Purpose in Existing Model	Limitations
Authentication Algorithm	Username-Password Based	Verifies user identity through a central server	Vulnerable to password theft and brute-force attacks
Symmetric Encryption	AES , DES	Encrypts data during transmission	Key management is centralized
Asymmetric Encryption	RSA	Secure key exchange and digital signatures	High computational cost
Hashing Algorithm	MD5 ,SHA	Ensures password security and data integrity	Weak against advanced attacks (MD5)
Firewall Algorithm	Rule-Based Filtering	Allows or blocks traffic	Cannot detect unknown

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, January 2026 Impact Factor: 7.67

		based on rules	attacks
Intrusion Detection Algorithm	Signature-Based IDS	Detects known attack patterns	Ineffective against new threats
Access Control Algorithm	Role-Based Access Control (IRBAC)	Manages user permissions centrally	Depends on trusted authority

In the existing traditional network security model, security is mainly based on centralized cryptographic and rule-based algorithms. The commonly used algorithms are:

• **Password-Based Authentication Algorithms:**Simple username–password verification algorithms are used to authenticate users through a central server.

• **Symmetric Encryption Algorithms (AES, DES):**Algorithms such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES) are used to encrypt and decrypt data during network communication.

• **Asymmetric Encryption Algorithms (RSA):**RSA algorithm is used for secure key exchange and digital signatures in centralized authentication systems.

• **Hashing Algorithms (MD5, SHA):**Hash functions like MD5 and SHA are used to store passwords and verify data integrity.

• **Rule-Based Firewall Algorithms**:Firewalls use predefined rule-based algorithms to allow or block network traffic based on IP address, port number, and protocol.

• **Signature-Based IDS Algorithms**:Intrusion Detection Systems (IDS) use signature-matching algorithms to detect known attack patterns.

These algorithms provide basic network protection but rely heavily on centralized control, making them vulnerable to single points of failure, insider attacks, and data tampering. This limitation motivates the shift toward blockchain-based decentralized security models.

VI. OUTPUT/RESULT AND DISCUSSION

Input Condition	System Output	Decision Taken
Valid User Credentials	Login Successful	Access granted
Invalid Credentials	Login Failure	Access denied
Encrypted data received	Data accepted	Data Forwarded securely
Unencrypted data detected	Security Alert Generated	Data Transmission Blocked
Known attack signature found	Attack Detected	Connection Terminated
Unknown Traffic Pattern	No Detection	Traffic allowed
Server Overload Condition	Response Delay	Request queued
Central server failure	System unavailable	Network access denied

The analysis of existing research and comparative study indicates that blockchain-based network security models provide significant improvements over traditional centralized security systems. The major outcome observed is the elimination of single points of failure due to the decentralized nature of blockchain. Unlike conventional models where security decisions are managed by a central server, blockchain distributes trust across multiple nodes, thereby enhancing system reliability and resilience.

The results show that blockchain-based authentication and access control mechanisms improve data integrity and transparency. Since all security-related events are recorded as immutable transactions, unauthorized data modification and insider attacks become easily detectable. Additionally, the use of cryptographic hashing and consensus mechanisms strengthens resistance against common cyber-attacks such as identity spoofing and data tampering.

However, the discussion also highlights certain limitations. Blockchain-based security models may introduce latency and increased computational overhead due to transaction validation and consensus processes. Scalability remains a challenge, particularly in large-scale network environments. Despite these issues, existing studies suggest that the

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, January 2026 Impact Factor: 7.67

advantages of enhanced security, transparency, and trust outweigh the performance limitations for small to medium-scale networks such as organizational or campus networks.

Overall, the results confirm that blockchain technology has strong potential to enhance network security. Further improvements can be achieved by adopting lightweight blockchain frameworks and integrating emerging technologies such as artificial intelligence to optimize performance and threat detection.

VII. CONCLUSION

This paper presented a comprehensive survey on the application of blockchain technology in network security. Traditional network security models rely on centralized architectures, which are vulnerable to single points of failure, trust issues, and various cyber-attacks. Through the analysis of existing research, it was observed that blockchain offers an effective solution to these challenges by providing decentralization, transparency, and data immutability.

The study highlighted how blockchain can enhance key security aspects such as authentication, access control, data integrity, and attack resistance. The comparative discussion demonstrated that blockchain-based security models improve trust and reliability in network environments compared to traditional approaches. Although challenges such as scalability, latency, and computational overhead still exist, these limitations can be addressed through lightweight blockchain frameworks and optimized consensus mechanisms.

Overall, blockchain technology shows strong potential to strengthen network security systems. With further research and integration with emerging technologies such as artificial intelligence and Internet of Things, blockchain-based security solutions can become more efficient, scalable, and suitable for real-world deployment in modern network environments.

REFERENCES

[1] S. Nakamoto, “Bitcoin**:** A Peer-to-Peer Electronic Cash System,” 2008.

[2] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” IEEE International Congress on Big Data, 2017.

[3] M. Conti, S. Kumar, C. Lal, and S. Ruj, “A Survey on Security and Privacy Issues of Bitcoin,” IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3416–3452, 2018.

[4] A. Dorri, S. S. Kanhere, and J. Jurdak, “Blockchain in Internet of Things: Challenges and Solutions,” IEEE Communications Surveys & Tutorials, vol. 19, no. 3, pp. 1731–1745, 2017.

[5] Y. Zhang, R. Yu, S. Xie, Y. Zhang, and M. Guizani, “HomeChain: A Blockchain-Based Secure Mutual Authentication System for Smart Homes,” IEEE Internet of Things Journal, 2018.

[6] W. Stallings, Cryptography and Network Security**:** Principles and Practice, 7th ed., Pearson Education, 2017.

[7] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, “On Blockchain and Its Integration with IoT: Challenges and Opportunities,” Future Generation Computer Systems, vol. 88, pp. 173–190, 2018.

[8] D. Tapscott and A. Tapscot**t**, Blockchain Revolution, Penguin Random House, 2016.

[9] Y. Zhang and J. Wen**, “**The IoT Electric Business Model: Using Blockchain Technology for the Internet of Things,” Peer-to-Peer Networking and Applications, vol. 10, no. 4, pp. 983–994, 2017.