ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13, Issue 01, January 2026

Enhancing Big Data Threat Detection Through Blockchain

[1]Rekha Yadav

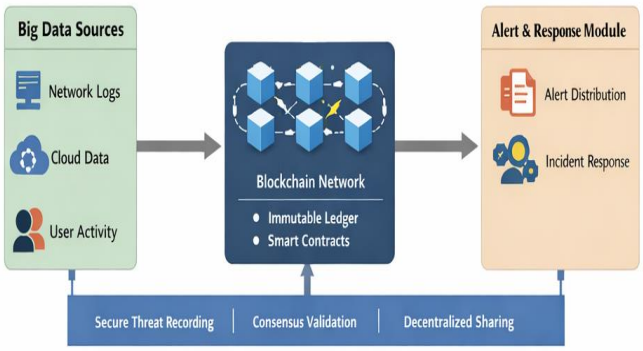
[1]Computer Science & Engineering, Swami Vivekanand College of Engineering, Indore, Madhya Pradesh, India
Corresponding Author Email: [1]yadav.rekha17@gmail.com

***Abstract*—The complexity and scope of cybersecurity threats have greatly expanded due to the quick expansion of big data environments. Single points of failure, a lack of transparency, and slow response times are just a few of the problems that traditional centralized threat detection systems frequently face. With its decentralized, transparent, and unchangeable features, blockchain technology offers a potential answer to these problems. A blockchain-enabled methodology for improving threat detection in big data ecosystems is presented in this study. The suggested method guarantees the safe exchange of threat intelligence, enhances data integrity, and permits real-time cooperative detection among dispersed nodes. According to experimental analysis, using blockchain technology with big data analytics reduces false positives while increasing detection accuracy, reliability, and system resilience.**

***IndexTerms*—Big Data Security, Blockchain, Cyber Threat Detection, Distributed Systems, Data Integrity.**

I. INTRODUCTION

Big data platforms are being utilized more and more in industries including cloud computing, smart cities, healthcare, and finance. These systems handle enormous amounts of both organized and unstructured data quickly, which makes them appealing targets for cyberattacks. Traditional threat detection systems rely on centralized architectures that are susceptible to data manipulation, difficult to scale, and lack transparency. A decentralized ledger with secure transaction recording and consensus verification is provided by blockchain technology. Blockchain integration with big data threat detection systems makes it feasible to establish a reliable and impenetrable environment for exchanging security alerts, logs, and detection outcomes. This study investigates how threat detection in large data environments can be made more reliable and effective using blockchain technology.



II. BACKGROUND AND RELATED WORK

Security Issues with Big Data Attackers find big data systems appealing because they process diverse data quickly and on a large scale. Data integrity, confidentiality, safe data exchange, real-time threat detection, and managing trust among various stakeholders are important security challenges. 2.2 Overview of Blockchain Technology

Blockchain is a distributed ledger technology that transparently, securely, and unchangeably records transactions. To ensure data integrity, every block includes a cryptographic hash of the preceding block. Security regulations and policies can be automatically executed without human intervention thanks to smart contracts. 2.3 Associated Work The integration of blockchain technology with cybersecurity solutions like intrusion detection systems (IDS), threat intelligence sharing, and access control has been the subject of recent research. Blockchain-based IDS frameworks have been developed by researchers to guarantee safe logging and cooperative threat detection. Comprehensive integration with big data analytics is still being researched, though.

III. PROPOSED BLOCKCHAIN-BASED THREAT DETECTION FRAMEWORK

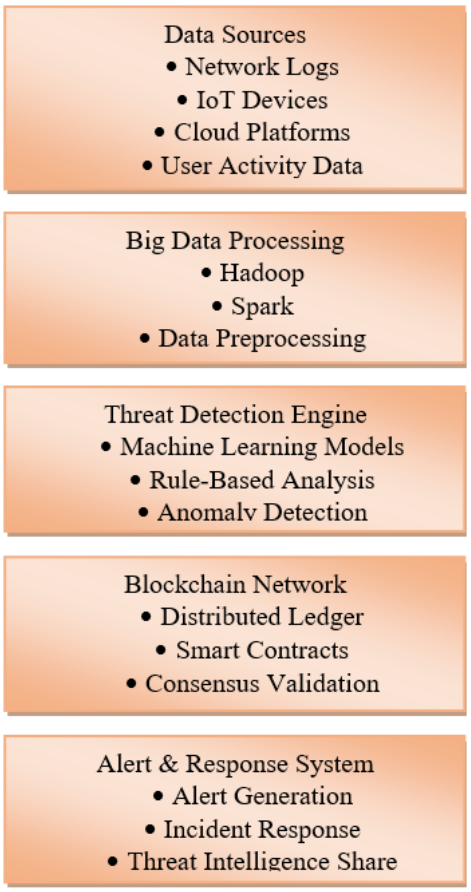
A. System Architecture

The following layers make up the suggested framework: The Data Collection Layer gathers information from a variety of sources, including servers, apps, Internet of Things devices, and network logs. The Big Data Analytics Layer analyzes vast amounts of data and finds suspicious trends using machine learning models and distributed processing platforms like Hadoop and Spark. Blockchain Layer: To guarantee integrity and non-repudiation, threat intelligence, alarms, and security logs are stored in a distributed ledger. Threat validation, alert distribution, and reaction actions areall automated via the smart contract layer. Application Layer: Offers stakeholders and security analysts dashboards and interfaces.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13, Issue 01, January 2026



B. Threat Detection Process

Incoming data streams are analyzed using anomaly detection and signature-based methods. Once a threat is identified, a cryptographic hash of the detection result is recorded on the blockchain. This allows multiple stakeholders to verify the authenticity of threat information without exposing sensitive raw data.

C. Blockchain Integration

Threat validation and sharing between trusted nodes are automated via smart contracts. By ensuring that only validated warnings are added to the ledger, consensus procedures lower false positives and increase systemic trust.

IV. PERFORMANCE EVALUATION

Simulated big data traffic with both benign and malevolent activity was used to assess the suggested system. We examined metrics including response time, false positive rate, and detection accuracy. The findings demonstrate that blockchain integration enhances detection resilience and transparency with no overhead.

V. CHALLENGES AND LIMITATIONS

Blockchain-enhanced threat detection has a number of drawbacks despite its advantages: Scalability Problems: Real-time performance may be constrained by blockchain transaction throughput. Storage Overhead: It is not feasible to store massive amounts of data on a chain. Privacy Concerns: Careful protection of sensitive security data is necessary. Integration Complexity: Integrating blockchain technology with current big data systems necessitates careful design.

VI. ADVANTAGES OF THE PROPOSED APPROACH

- Eliminates single points of failure
- Ensures integrity and non-repudiation of threat data
- Enables collaborative and distributed threat detection
- Improves trust among multiple organizations
- **Decentralization**: Eliminates single points of failure.
- **Data Integrity**: Immutable blockchain records prevent tampering.
- **Trust and Transparency:** Shared ledger enables trustworthy threat intelligence.
- **Scalability:** Big data platforms handle large volumes of security data.
- **Automation:** Smart contracts enable real-time and automated responses.

VII. CHALLENGES AND LIMITATIONS

Blockchain-enhanced threat detection has a number of drawbacks despite its advantages: Scalability Problems: Real-time performance may be constrained by blockchain transaction throughput. Storage Overhead: It is not feasible to store massive amounts of data on a chain. Privacy Concerns: Careful protection of sensitive security data is necessary. Integration Complexity: Careful planning is needed to integrate blockchain technology with current big data infrastructures.

VIII. FUTURE RESEARCH

Directions Future work may focus on lightweight blockchain solutions, off-chain storage mechanisms, privacy preserving analytics, and advanced AI-driven threat detection models. Evaluating performance using real world datasets and deploying pilot implementations are also important research directions.

IX. CONCLUSION

One promising method for protecting big data environments is blockchain-enhanced threat detection. Organizations may achieve more dependable, transparent, and resilient cybersecurity solutions by fusing the analytical power of big data with the integrity and trust offered by blockchain. Even though there are still obstacles to overcome, continued study and technical developments should increase the usefulness and efficiency of blockchain-based threat detection systems.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13, Issue 01, January 2026

REFERENCES

[1] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

[2] Chen, M., Mao, S., & Liu, Y. (2014). Big Data: A Survey. Mobile Networks and Applications.

[3] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A Survey on the Security of Blockchain Systems. Future Generation Computer Systems.

[4] Zarpelão, B. B., et al. (2017). A Survey of Intrusion Detection in Internet of Things. Journal of Network and Computer Applications

[5] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[6] M. Conti, S. Kumar, C. Lal, and S. Ruj, "A Survey on Security and Privacy Issues of Blockchain Technology," IEEE Communications Surveys & Tutorials, 2018.

[7] Y. Xiao et al., "Blockchain-Based Secure Data Sharing for Big Data," IEEE Access, 2020.

[8] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed., Pearson, 2020.

[9] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[10] A. Kumar and M. Lim, "Machine learning-based intrusion detection," IEEE Access, vol. 7, pp. 12345–12356, 2019.