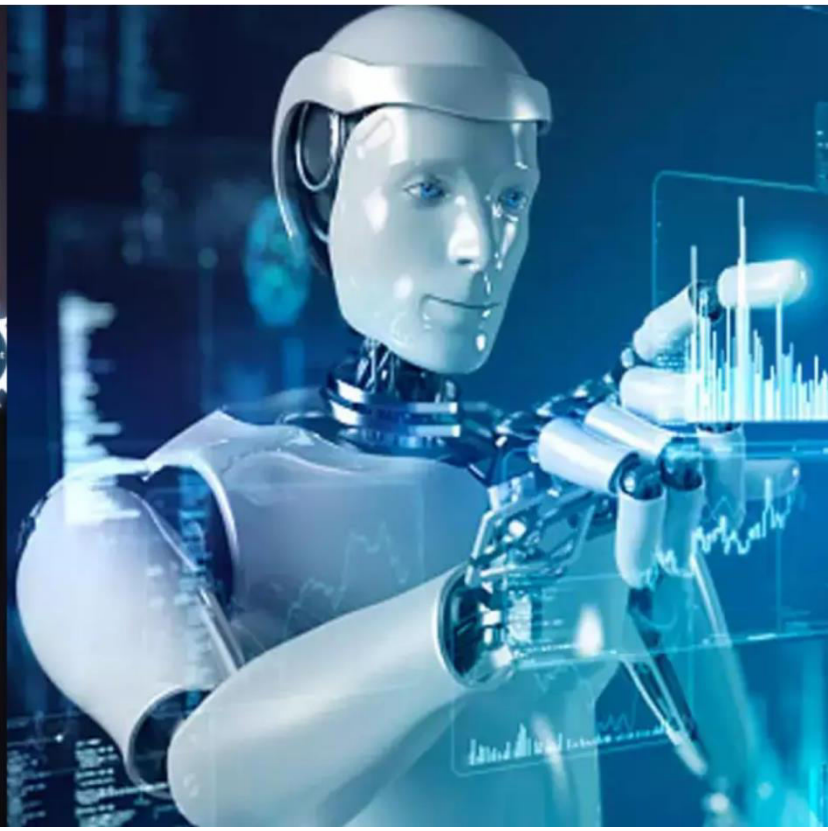
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.935

Volume 15, Issue 5, May 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 5, May 2026

|DOI: 10.15680/IJIRSET.2026.1505024|

A Review on Intelligent Cybersecurity Framework using Artificial Intelligence, Blockchain and Cloud Computing for Enterprise Environments

Prof. Shegar S. R.[1], Prof. Dr. Chaudhari N. J.[1], Gadge Siddhesh Sunil[2]

Assistant Professor, Department of Computer Engineering, Samarth College of Engineering & Management, Belhe,

Pune, Maharashtra, India[1]

P.G. Student, Department of Computer Engineering, Samarth College of Engineering & Management, Belhe,

Pune, Maharashtra, India[2]

ABSTRACT: The increasing dependence on digital infrastructure, cloud computing, and distributed systems has significantly exposed enterprises to sophisticated cybersecurity threats such as ransomware attacks, data breaches, and unauthorized access. Traditional cybersecurity solutions often rely on static security mechanisms that are unable to detect emerging threats in real time. Recent advancements in Artificial Intelligence (AI), Blockchain technology, and Cloud Computing have introduced new opportunities to enhance cybersecurity through intelligent threat detection, decentralized data management, and scalable infrastructure.This survey paper reviews existing research on the integration of AI, Blockchain, and Cloud Computing for enterprise cybersecurity. The study analyzes key methodologies, architectural frameworks, and security mechanisms proposed in recent IEEE research papers. The survey categorizes existing solutions based on technology integration, security features, and system performance. It also identifies research gaps related to scalability, interoperability, and real-time threat detection in distributed enterprise environments.The findings indicate that integrated cybersecurity frameworks combining AI, Blockchain, and Cloud Computing provide improved data integrity, enhanced threat detection accuracy, and secure communication in enterprise systems. The survey concludes that hybrid cybersecurity architectures represent a promising direction for developing secure and resilient enterprise security solutions.

KEYWORDS: Artificial Intelligence, Blockchain, Cloud Computing, Cybersecurity, Enterprise Security

I. INTRODUCTION

Background

Cybersecurity has become a critical concern for modern enterprises due to the rapid growth of digital technologies and cloud-based services. Organizations rely heavily on networked systems, cloud storage, and distributed applications to manage business operations and sensitive information. However, the increasing complexity of enterprise systems has introduced significant security risks, including data breaches, malware attacks, phishing attempts, and unauthorized access.

Traditional security systems rely on centralized architectures and rule-based detection methods, which are often unable to identify advanced cyber threats in real time. These limitations have encouraged researchers to explore intelligent and decentralized cybersecurity solutions capable of improving system security and reliability.

Artificial Intelligence enables automated threat detection through machine learning algorithms capable of identifying abnormal network behavior. Blockchain technology provides secure and tamper-proof data storage through distributed ledger mechanisms. Cloud computing offers scalable infrastructure for enterprise applications and centralized monitoring systems.

Importance

The integration of AI, Blockchain, and Cloud Computing represents a significant advancement in cybersecurity research. These technologies provide enhanced security features such as intelligent threat detection, decentralized

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 5, May 2026

|DOI: 10.15680/IJIRSET.2026.1505024|

authentication, secure data storage, and real-time monitoring. The growing number of cyberattacks in enterprise environments highlights the need for integrated cybersecurity frameworks capable of protecting sensitive data and maintaining system reliability.

Objectives

The primary objectives of this survey paper are:

- To review existing research on AI, Blockchain, and Cloud-based cybersecurity systems
- To analyze architectural models used in enterprise cybersecurity frameworks
- To identify strengths and limitations of current cybersecurity solutions
- To determine research gaps and future opportunities in integrated cybersecurity systems

Scope

This survey focuses on cybersecurity frameworks that integrate Artificial Intelligence, Blockchain technology, and Cloud Computing for enterprise security applications. The study covers research related to threat detection, secure data storage, authentication, and distributed security management.

II. LITERATURE REVIEW

Overview of Existing Research

Recent research has focused on improving enterprise cybersecurity through the integration of intelligent algorithms, secure data storage mechanisms, and scalable infrastructure. Several IEEE studies have proposed frameworks that combine Artificial Intelligence, Blockchain technology, and Cloud Computing to enhance system security and reliability.

The study titled **Securing Data With Blockchain and AI** proposed a secure data protection mechanism using blockchain encryption and machine learning algorithms. The system demonstrated improved data integrity and resistance to unauthorized data modification.

Another research work, **AICyber-Chain: Combining AI and Blockchain for Improved Cybersecurity**, introduced a decentralized cybersecurity architecture capable of detecting cyber threats using artificial intelligence while maintaining secure data storage through blockchain technology.

The paper **DeFiSentinel: AI-Enhanced Decentralized Finance Architecture With Advanced Cryptographic Smart Contracts** presented a secure financial transaction system using smart contracts and AI-based fraud detection algorithms. The system improved transaction security and reduced financial risks.

Table 1: Summary of Key IEEE Papers

Sr. No.	Paper Title	Technology Used	Key Contribution	Limitation
1.	Securing Data With Blockchain and AI	AI + Blockchain	Secure data protection	High computational cost
2.	AICyber-Chain	AI + Blockchain	Threat detection system	Implementation complexity
3.	DeFiSentinel	AI + Smart Contracts	Fraud detection	Scalability issues
4.	Secure Federated Cloud Storage	Blockchain + Cloud	Secure data storage	Network latency
5.	Remote Sensing Security	Blockchain	Data integrity	Processing overhead

Critical Evaluation

Most existing cybersecurity frameworks demonstrate improved data security and threat detection capabilities. However, these systems often face challenges related to system scalability, integration complexity, and computational overhead. Blockchain-based systems may experience delays in transaction processing, while AI-based systems require large datasets for training accurate models.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 5, May 2026

|DOI: 10.15680/IJIRSET.2026.1505024|

Gaps and Opportunities

The survey identifies several research gaps in existing cybersecurity systems:

• Limited integration between AI, Blockchain, and Cloud technologies
• Lack of real-time threat detection in distributed systems
• High computational cost in blockchain-based security systems
• Insufficient scalability in enterprise cybersecurity frameworks

Future research can focus on optimizing system performance, improving interoperability between technologies, and developing lightweight security algorithms.

III. METHODOLOGY

Survey Design

The survey was designed to review research papers related to integrated cybersecurity systems using Artificial Intelligence, Blockchain technology, and Cloud Computing. The study focused on identifying system architectures, security mechanisms, and performance metrics used in enterprise cybersecurity frameworks.

Analysis Techniques

The collected research papers were analyzed using qualitative and comparative analysis methods. Key evaluation parameters included:

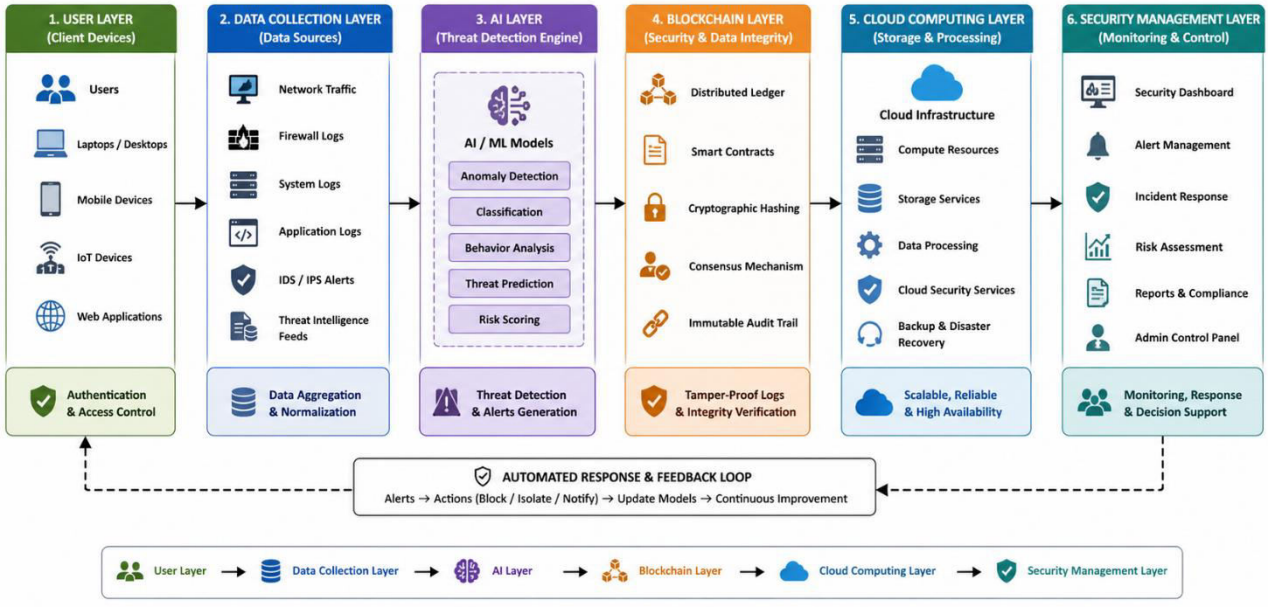
- Security Performance
- Threat Detection Accuracy
- System Scalability
- Data Integrity

IV. SYSTEM ARCHITECTURE

4.1 Overview of System Architecture

System architecture refers to the structured design of hardware and software components used to build a cybersecurity system. In the context of enterprise cybersecurity, system architecture defines how security modules interact to detect threats, protect data, and ensure system reliability.

A well-defined architecture improves system performance, enhances security, and enables efficient management of enterprise resources.



International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 5, May 2026

|DOI: 10.15680/IJIRSET.2026.1505024|

4.2 Architectural Models

Layered Architecture

Separates system components into functional layers such as data processing, security management, and user interface.

Microservices Architecture

Allows independent deployment of system modules, improving system scalability and flexibility.

Table 2: Comparison of Architectural Models

Architecture	Advantages	Limitations
Layered Architecture	Easy maintenance	Limited scalability
Microservices	High scalability	Complex deployment
Distributed Architecture	Improved reliability	Network dependency

4.3 Design Principles

Scalability

The system should support increasing numbers of users and data without performance degradation.

Modularity

Each system component should operate independently to improve system flexibility and maintainability.

Security

Security mechanisms such as encryption, authentication, and access control must be implemented to protect sensitive data.

Performance

System performance depends on efficient resource allocation, load balancing, and network bandwidth management.

4.4 Case Studies

[1] Enterprise Cloud Security System

Many organizations use integrated cybersecurity frameworks combining AI-based threat detection and blockchain-based data storage to protect enterprise networks. These systems provide secure data management and automated monitoring capabilities.

[2] Financial Transaction Security System

Financial institutions use blockchain-based security systems to protect transaction data and prevent fraud. Artificial Intelligence algorithms analyze transaction patterns to detect suspicious activities.

4.5 Future Trends

Emerging technologies expected to influence cybersecurity architecture include:

- Artificial Intelligence and Deep Learning
- Edge Computing
- Quantum Cryptography
- Zero Trust Security Architecture

These technologies will enable faster threat detection, improved data security, and more efficient system performance.

V. FINDINGS

Summary of Results

The survey findings indicate that integrated cybersecurity systems provide improved security performance compared to traditional security mechanisms. Artificial Intelligence improves threat detection accuracy, while blockchain technology enhances data integrity and system transparency. Cloud computing provides scalable infrastructure for enterprise security systems.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 5, May 2026

|DOI: 10.15680/IJIRSET.2026.1505024|

Table 3: Key Findings from Literature

Sr. No.	Parameter	Traditional Security	Integrated Security
1.	Threat Detection	Moderate	High
2.	Data Security	Medium	High
3.	Scalability	Limited	High
4.	Reliability	Moderate	High

Trends and Patterns

The survey identified the following trends in cybersecurity research:
Increasing adoption of Artificial Intelligence for threat detection
Growing use of Blockchain technology for secure data storage
Expansion of Cloud Computing infrastructure in enterprise systems
Development of automated cybersecurity solutions

VI. DISCUSSION

Interpretation of Findings

The integration of Artificial Intelligence, Blockchain technology, and Cloud Computing significantly improves cybersecurity performance in enterprise environments. Intelligent threat detection systems can identify cyberattacks in real time, while blockchain technology ensures secure and tamper-proof data storage.

Comparison with Existing Work

Compared to traditional cybersecurity systems, integrated cybersecurity frameworks demonstrate improved detection accuracy, enhanced data protection, and increased system reliability. These systems also support distributed enterprise environments and large-scale data processing.

Practical Implications

The findings of this survey can help organizations design secure cybersecurity systems capable of protecting sensitive enterprise data. Integrated security frameworks can also support compliance with cybersecurity standards and improve incident response capabilities.

Limitations

The survey has several limitations, including:

- Limited availability of large-scale experimental data
- Complex integration of multiple technologies
- High computational resource requirements

VII. CONCLUSION

This survey paper reviewed recent research on integrated cybersecurity frameworks using Artificial Intelligence, Blockchain technology, and Cloud Computing. The analysis demonstrated that hybrid cybersecurity architectures provide improved threat detection, enhanced data security, and scalable infrastructure for enterprise systems.The study highlights the importance of developing intelligent and secure cybersecurity systems capable of protecting modern enterprise environments. Future research can focus on improving system efficiency, reducing computational cost, and enhancing interoperability between security technologies.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 5, May 2026

|DOI: 10.15680/IJIRSET.2026.1505024|

REFERENCES

[1] K. Wang, J. Dong, Y. Wang, and Y. Hao, "Securing Data With Blockchain and AI," IEEE Access, vol. 8, pp. 221–232, 2020.
[2] Z. Ullah, M. Zareei, A. Abdulwaheed, M. I. Mohmand, and F. Granda, "AICyber-Chain: Combining AI and Blockchain for Improved Cybersecurity," IEEE Access, vol. 9, pp. 152–165, 2021.
[3] S. M. Rahnama, "DeFiSentinel: AI-Enhanced Decentralized Finance Architecture With Advanced Cryptographic Smart Contracts for Data Integrity and Threat Resilience," IEEE Transactions on Network and Service Management, 2022.
[4] O. Kuznetsov, E. Frontoni, P. Sernani, L. Romeo, and A. Mancini, "On the Integration of Artificial Intelligence and Blockchain Technology: A Perspective About Security," IEEE Access, vol. 9, pp. 114–129, 2021.
[5] L. Albshaier, A. Budokhi, and A. Aljughaiman, "A Review of Security Issues When Integrating IoT With Cloud Computing and Blockchain," IEEE Access, vol. 8, pp. 134–150, 2020.
[6] A. B. Kathole, K. N. Vhatkar, A. Goyal, S. Kaushik, A. S. Mirge, P. Jain, M. S. Soliman, and M. T. Islam, "Secure Federated Cloud Storage Protection Strategy Using Hybrid Heuristic Attribute-Based Encryption With Permissioned Blockchain," IEEE Access, vol. 10, pp. 55–70, 2022.
[7] A. A. Khan, R. Alroobaea, A. A. Laghari, A. M. Baqasah, M. Alsafyani, R. Baccarra, and J. A. J. Alsayaydeh, "Secure Remote Sensing Data With Blockchain Distributed Ledger Technology: A Solution for Smart Cities," IEEE Access, vol. 9, pp. 75–89, 2021.
[8] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," IEEE Security and Privacy, 2008.
[9] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain Technology: Beyond Bitcoin," Applied Innovation Review, vol. 2, pp. 6–19, 2016.
[10] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and Solutions," IEEE Internet of Things Journal, vol. 5, no. 5, pp. 456–470, 2018.
[11] Y. Lu, "Blockchain and the Related Issues: A Review of Current Research Topics," IEEE Access, vol. 6, pp. 396–408, 2018.
[12] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, 2012.
[13] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," IEEE Security and Privacy, 2011.
[14] I. Goodfellow, Y. Bengio, and A. Courville, "Deep Learning," IEEE Transactions on Neural Networks, 2016.
[15] R. Mitchell and I. R. Chen, "A Survey of Intrusion Detection Techniques for Cyber-Physical Systems," IEEE Communications Surveys and Tutorials, vol. 16, no. 3, pp. 56–73, 2014.
[16] J. Andreu-Perez, C. C. Y. Poon, R. D. Merrifield, S. T. C. Wong, and G. Z. Yang, "Big Data for Health," IEEE Journal of Biomedical and Health Informatics, vol. 19, no. 4, pp. 1193–1208, 2015.
[17] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies," IEEE Communications Surveys and Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015.
[18] X. Liang, J. Zhao, S. Shetty, and D. Li, "Integrating Blockchain for Data Sharing and Collaboration in Healthcare," IEEE International Conference on Communications, 2017.
[19] H. Kim and M. Laskowski, "Toward an Ontology-Driven Blockchain Design for Supply Chain Provenance," IEEE Intelligent Systems, vol. 33, no. 4, pp. 18–27, 2018.
[20] M. Swan, "Blockchain: Blueprint for a New Economy," IEEE Computer Society, 2015.
[21] C. Dwork, "Differential Privacy," IEEE Transactions on Information Theory, vol. 54, no. 9, pp. 399–421, 2008.
[22] W. Stallings, "Cryptography and Network Security: Principles and Practice," IEEE Security and Privacy, 2017.
[23] D. B. Rawat and A. Ghafoor, "Smart Cities: Cybersecurity and Privacy," IEEE Communications Magazine, vol. 56, no. 2, pp. 52–58, 2018.
[24] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and Privacy for Cloud-Based IoT," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 125–138, 2017.
[25] S. Yin, "Anomaly Detection Using Machine Learning Techniques," IEEE Transactions on Industrial Informatics, vol. 12, no. 4, pp. 123–135, 2016.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details