A Survey On Blockchain-Based Cybersecurity for IoT Devices

Anushka Sankpal
Master Of Computer Application,
KLS Gogte Institute Of Technology
Belgaum, India
Email:2gi23mc014@students.git.edu

Pipreeta Chougule
Master Of Computer Application,
KLS Gogte Institute Of Technology
Belgaum, India
Email:2gi23mc061@students.git.edu

Mrutyunjaya S Emmi
Master Of Computer Application,
KLS Gogte Institute Of Technology
Belgaum, India

***Abstract*—The cybersecurity domain surrounding the Internet of Things (IoT) and Industrial Internet of Things (IIoT) is rapidly evolving, driven by the fusion of blockchain technology and artificial intelligence (AI). This review comprehensively analyzes current research focused on integrating blockchain and AI to bolster intrusion detection systems (IDS) and overall security mechanisms in IoT environments. Following the PRISMA methodology, this study scrutinizes over one hundred peer-reviewed articles published between 2019 and 2024. It identifies key technological trends, research methods, and prevailing challenges while proposing a conceptual framework for creating decentralized and intelligent IDS solutions. The paper pays special attention to emerging areas such as lightweight cryptographic methods, post-quantum cryptography (PQC), and explainable AI (XAI). This review aims to serve as a robust reference for researchers and industry experts aspiring to develop secure, intelligent, and scalable IoT infrastructures.**

***Index Terms*—Blockchain, Artificial Intelligence, Internet of Things, Industrial IoT, Cybersecurity, Intrusion Detection Systems, Federated Learning, Post-Quantum Cryptography, Explainable AI**

I. Introduction

In recent years, IoT has become a ubiquitous part of our lives, connecting everything from home appliances and wearable devices to industrial machinery and smart city infrastructure. While this evolution brings greater convenience and innovation, it also opens the door to new types of cyber threats. Each IoT device acts as a potential point of vulnerability, and securing these devices—many of which are resource-constrained—is becoming increasingly difficult with traditional tools [4], [9].

The Industrial Internet of Things (IIoT) raises the stakes even further, where failure or security breaches can directly impact critical infrastructure like energy grids, manufacturing lines, and healthcare systems. Traditional intrusion detection systems, especially those relying on static signatures, often fail to keep pace with evolving threats [4], [9].

Enter blockchain and artificial intelligence—two transformative technologies that, when combined, offer the promise of smarter, decentralized, and adaptive security mechanisms. Blockchain provides immutable records, decentralization, and smart contract automation [1], [2], [6], while AI offers real-time threat detection and predictive analytics [7], [10]. Together, they provide a new lens through which we can reimagine cybersecurity for the IoT era.

The stakes are particularly high in the IIoT domain, where security breaches or system failures can have catastrophic consequences, directly impacting critical infrastructure such as energy grids, manufacturing lines, and healthcare systems. Conventional intrusion detection systems (IDS), often reliant on static signatures, struggle to keep pace with the dynamic and rapidly evolving threat landscape. This inadequacy necessitates a paradigm shift in cybersecurity approaches for IoT environments.

II. Research Methodology

To ensure the reliability and comprehensiveness of this review, we used the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework. We sourced articles from leading databases such as IEEE Xplore, SpringerLink, ACM Digital Library, MDPI, and arXiv, focusing on work published between 2019 and 2024 [3], [6], [9].

An initial search yielded 189 articles. After eliminating duplicates, filtering non-English documents, and removing inaccessible full texts, we were left with 167. A relevance screening removed papers that didn't specifically discuss AI, blockchain, and IoT/IIoT security intersections. A final selection of 111 high-quality papers was analyzed and categorized according to their methods, contributions, and technical focus.

The initial phase involved a comprehensive search across leading academic databases renowned for their coverage of computer science, engineering, and cybersecurity literature. These databases included:

- IEEE Xplore: A vast repository of publications from the Institute of Electrical and Electronics Engineers, covering a broad spectrum of technology.
- SpringerLink: Offering access to journals, books, and proceedings across various scientific disciplines.
- ACM Digital Library: The full-text collection of publications from the Association for Computing Machinery, a key resource for computer science research.
- MDPI (Multidisciplinary Digital Publishing Institute): A publisher of open-access journals across numerous scientific and technical fields.

- arXiv: An open-access archive for preprints of scientific papers, providing early access to cutting-edge research.

The search strategy was specifically designed to capture the most recent advancements, focusing exclusively on peer-reviewed articles published between 2019 and 2024. This timeframe was chosen to reflect the rapid evolution of both blockchain and AI technologies and their application in IoT security.

An initial broad search using relevant keywords (e.g., ”blockchain,” ”artificial intelligence,” ”IoT security,” ”IIoT cybersecurity,” ”intrusion detection systems”) yielded a substantial pool of 189 articles. The subsequent stages involved a rigorous filtering process:

1) Duplicate Removal: All duplicate entries identified across the various databases were systematically eliminated to ensure each unique study was considered only once.
2) Language Filtering: To maintain consistency and facilitate in-depth analysis, only English-language documents were retained.
3) Accessibility Check: Papers for which full-text access could not be obtained were excluded, as their content could not be thoroughly reviewed.

III. Thematic Insights

A. Blockchain Applications in IoT Security

Blockchain’s core attributes—decentralization, transparency, and immutability—make it an attractive solution for enhancing IoT security [4]. Traditional centralized systems face vulnerabilities due to single points of failure, whereas blockchain distributes control across a peer-to-peer network, reducing such risks.

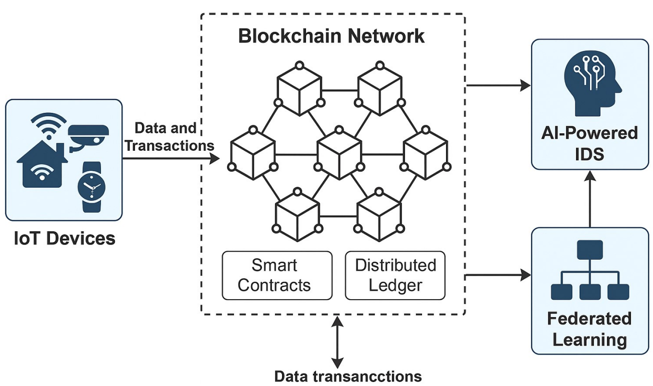

Fig. 1. Integrated Blockchain Architecture for IoT Security

In IoT environments, blockchain can be leveraged to monitor device interactions, enforce authentication processes, and facilitate secure firmware updates. Moreover, smart contracts can automate responses to specific conditions, such as isolating compromised devices or executing system patches.

However, resource constraints in IoT devices pose challenges for full-scale blockchain integration. To address this, lightweight consensus algorithms such as Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and hybrid blockchains are being explored [5], [13].

B. AI-Enhanced Intrusion Detection Systems

AI technologies, particularly machine learning (ML) and deep learning (DL), empower IDS to adaptively detect complex cyber threats [5]. Unlike traditional systems, AI models learn from historical data and can identify unknown or emerging attack patterns. Techniques such as Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, and reinforcement learning are utilized to recognize abnormal traffic behaviors.

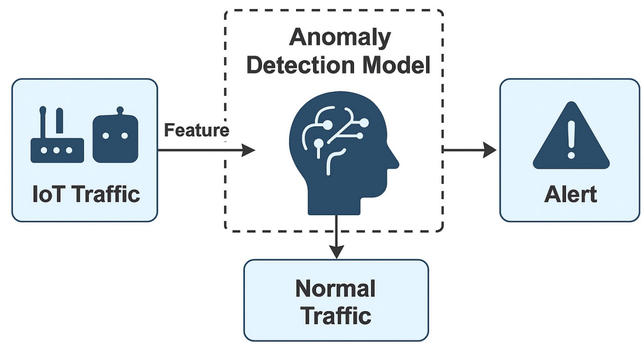

Fig. 2. AI-Driven IDS Framework for IoT Networks

AI also enables real-time threat analysis and autonomous decision-making. The increasing focus on Explainable AI (XAI) allows systems to justify their actions, which is crucial for applications in highly regulated industries. Nevertheless, AI-based systems face challenges related to data privacy, adversarial attacks, and high computational demands [10].

C. Converging Blockchain and AI for IoT Defense

The synergy between blockchain and AI creates a resilient cybersecurity framework [6]. While blockchain ensures data integrity and secure sharing, AI provides dynamic analysis and threat response capabilities. For instance, AI algorithms can analyze blockchain-stored logs for signs of malicious activities, and blockchain can securely disseminate these alerts across networks.

Federated Learning (FL) is another promising development. It enables decentralized AI model training across multiple devices while preserving data privacy. Blockchain acts as the coordinator, validating and aggregating local updates in a transparent and tamper-resistant manner [10], [12].

IV. Key Challenges

Despite its potential, the combined use of AI and blockchain in IoT security introduces several hurdles [7]:

- **Resource Constraints:** Most IoT devices have limited computational power, memory, and energy supply. Running AI models or maintaining a blockchain ledger can be unrealistic without optimized, lightweight versions.

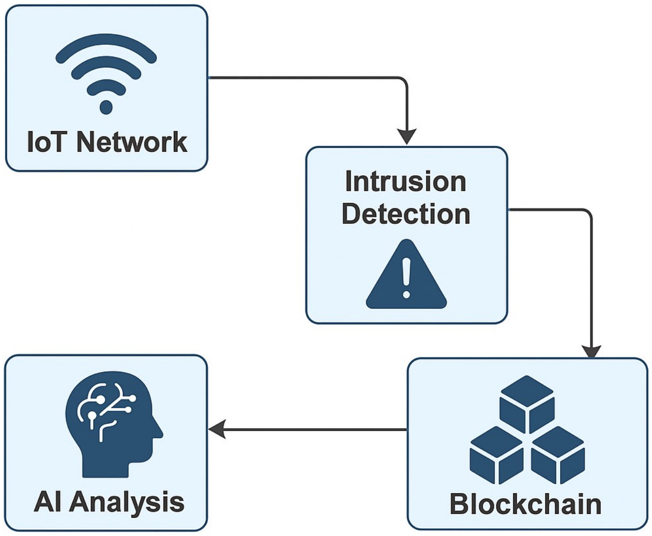

Fig. 3. Integrated AI-Blockchain Governance Workflow for Intrusion Detection

- AI Models: Complex AI models need more processing capacity and memory than most devices can provide, making on-device training impractical.
- Blockchain Ledgers: Full blockchain ledgers exceed the capabilities of typical IoT devices, requiring highly optimized versions for effective operation.
- Implication: Development of lightweight AI algorithms and blockchain protocols is essential to fit within device limitations.

- **Scalability:** As IoT networks grow, blockchain's data replication and consensus mechanisms can create bottlenecks. Achieving real-time threat detection becomes increasingly difficult.
  - Blockchain Bottlenecks: The design of blockchain can slow down transaction speeds, hindering performance as usage expands.
  - Real-time Threat Detection: High latency in blockchain can impair proactive cybersecurity measures.
  - Data Volume: The massive data generated by IoT presents storage and processing challenges for both AI and blockchain.
- **Privacy:** Blockchain's transparency, while a strength, can inadvertently expose sensitive metadata. Federated learning offers a partial solution, but even model parameters can be exploited [11].
  - Metadata Exposure: Public blockchain transparency can reveal metadata that may expose sensitive patterns and behaviors.
  - Federated Learning Limitations: Although it retains data locally, shared model parameters can still pose privacy risks.
- **Quantum Threats:** Quantum computers threaten traditional cryptographic systems. Post-quantum cryptography (PQC) aims to future-proof blockchain, but implementations remain in early stages [13].
  - Cryptographic Vulnerability: Many current algorithms may be broken by quantum computers, endangering the security of IoT communications and transactions.
  - Post-Quantum Cryptography (PQC): Integration of PQC into current systems is complex and requires significant effort.
- **Standardization and Interoperability:** A lack of unified protocols makes it difficult to deploy integrated solutions across different IoT ecosystems. Governance models for these decentralized systems also need development.
  - Fragmented Ecosystems: Proprietary protocols create challenges in communication and data sharing among different platforms.
  - Governance Models: Developing clear governance for decentralized systems integrating AI is complex, lacking clear guidelines.
  - Regulatory Landscape: Evolving data privacy regulations complicate standardization and adaptability of solutions.

V. Innovations and Trends

Innovative trends are helping to overcome these challenges [8]:

- **Blockchain-as-a-Service (BaaS):** Major providers like AWS, Microsoft Azure, and IBM now offer BaaS platforms that allow developers to implement blockchain functionality without deep expertise or large infrastructure [1].
  - Democratization: Major cloud providers (AWS, Azure, IBM) offer BaaS, easing blockchain access.
  - Simplified Deployment: Enables blockchain functions without extensive expertise or upfront costs.
  - Managed Services: Provides support for setup, security, and scaling, reducing operational burdens.
- **Post-Quantum Cryptography (PQC):** Lattice-based and multivariate polynomial cryptographic methods are gaining traction to safeguard systems against future quantum attacks.
  - New Algorithms: Focuses on quantum-resistant algorithms like lattice-based and multivariate cryptography.
  - Future Protection: Essential for integrating PQC into blockchain and IoT to prevent quantum attacks.
  - Standardization: Efforts by NIST aim for the widespread adoption of PQC algorithms.
- **Edge Computing:** By processing data locally on edge devices, latency is reduced and privacy is improved. When coupled with lightweight AI models and blockchain nodes, edge computing enables real-time decision-making.
  - Local Processing: Computes data closer to IoT devices, reducing latency for real-time threat responses.

- Improved Privacy: Sensitive data stays local, aligning with federated learning techniques.
  - Distributed Intelligence: Combines lightweight AI and optimized blockchain at the network edge.
- **Smart Contract Automation:** These contracts now handle complex IoT workflows—from device authentication to automatic threat response. Improvements in formal verification tools ensure smart contracts are secure and reliable.
  - Complex Workflows: Evolve to automate security tasks, like device access management based on AI detections.
  - Formal Verification: Enhancements in verification tools ensure smart contracts are secure and reliable.
- **Interoperability Frameworks:** Initiatives like Polkadot, Cosmos, and Hyperledger are building the foundations for blockchain systems that can communicate across platforms, bridging gaps between fragmented IoT systems [13].
  - Cross-Chain Communication: Initiatives like Polkadot and Hyperledger enable seamless interaction across blockchains.
  - Unified Ecosystem: Aims to connect diverse IoT systems for improved security intelligence and coordinated responses.
  - Standardized APIs: Development of protocols is critical for achieving interoperability.

VI. Comparative Case Studies

TABLE I
COMPARATIVE ANALYSIS OF BLOCKCHAIN-AI IOT SECURITY SOLUTIONS

Case Study	Architecture	Strengths	Limitations
CNN + Blockchain + SDN	AI + SDN + Private Blockchain	Accurate, adaptable	Resource intensive
Federated Learning + Blockchain	FL + Blockchain + Smart Contracts	Privacy-preserving, efficient	Complex coordination
Healthcare IoT Security	Ethereum + IPFS + AI	Regulatory compliance, secure data	Scalability issues
Smart Grid Security	RL Agents + Blockchain	Autonomous, resilient	Computationally heavy

VII. Research Opportunities and Future Directions

Several promising areas for future research include [9]:

- **Lightweight Consensus Mechanisms:** More research is needed on consensus protocols that balance energy efficiency with security.
  - Energy Efficiency: Focus on protocols that extend battery life.
  - Low Computational Overhead: Aim for minimal processing requirements.
  - Scalability: Ensure protocols handle billions of devices and high transaction volumes securely.
  - Hybrid Approaches: Explore combining strengths of various consensus models.
- **Quantum-Safe Implementations:** PQC schemes must be adapted for IoT environments and tested for real-world performance.
  - Adaption: Tailor PQC schemes for IoT constraints (e.g., smaller keys).
  - Performance Testing: Evaluate PQC algorithms in real-world IoT scenarios.
  - Standardization: Ensure interoperability of different PQC implementations.
  - Migration Strategies: Develop secure transition methods to quantum-safe systems.
- **Explainable AI (XAI):** More interpretable AI models are essential for trust and accountability in critical systems.
  - Interpretable Models: Create clearer AI models for intrusion detection.
  - Post-hoc Explanations: Develop methods for understandable model decisions.
  - Human-in-the-Loop Systems: Enable human operators to verify AI insights.
  - Contextual Explanations: Ensure relevance of explanations to IoT contexts.
- **Benchmarking and Datasets:** Standard testbeds and metrics would help validate solutions and foster comparative research.
  - Standardized Datasets: Create diverse datasets for various IoT traffic and attack patterns.
  - Benchmarking Frameworks: Define metrics for evaluating performance and security.
  - Open-Source Testbeds: Establish environments for reproducible solution testing.
- **Ethical and Governance Frameworks:** Issues around data ownership, consent, and algorithmic bias must be addressed.
  - Data Ownership: Clarify data ownership and consent in decentralized settings.
  - Algorithmic Bias: Investigate and mitigate biases in AI decision-making.
  - Accountability: Define responsibility when AI makes autonomous security decisions.
  - Regulatory Compliance: Ensure adherence to data privacy laws across regions.
- **Human-Centric Design:** Understanding how users interact with and trust AI-blockchain systems is crucial for adoption.
  - User Interface/Experience (UI/UX): Design accessible interfaces for broader user adaptability.
  - Trust and Adoption: Study psychological factors affecting user trust in these systems.
  - Resilience to Human Error: Create systems robust to human misconfiguration or intervention.

VIII. Conclusion

As the digital ecosystem of IoT and IIoT continues to expand in both scale and complexity, safeguarding these systems against emerging cybersecurity threats has become more critical than ever. The convergence of blockchain and artificial intelligence represents a groundbreaking shift in how we approach these challenges. Through decentralization, transparency, and automation, blockchain ensures that data transactions and device interactions are secure, verifiable, and tamper-proof. At the same time, AI introduces the capacity for intelligent threat detection, adaptive learning, and autonomous decision-making.

This review offers an in-depth, human-centric exploration of the current landscape, analyzing over 100 peer-reviewed sources using the PRISMA framework. We examined foundational concepts, innovative trends like Blockchain-as-a-Service (BaaS), post-quantum cryptography, and federated learning, and identified practical case studies across healthcare, smart grids, and industrial automation. These studies demonstrate how real-world implementations are leveraging the synergy of blockchain and AI to detect intrusions, manage sensitive data, and ensure operational integrity in resource-constrained environments [1], [3].

Our analysis highlights key limitations such as resource inefficiencies, lack of standardization, quantum vulnerabilities, and usability concerns. Furthermore, the need for explainable AI (XAI), lightweight consensus algorithms, and ethical governance frameworks remains largely unmet [4], [5]. These gaps present substantial opportunities for interdisciplinary research and real-world deployment pilots.

Moving forward, the path to securing IoT systems lies not only in refining technologies but also in designing systems that prioritize user trust, ethical compliance, and sustainable deployment. Collaboration among technologists, policymakers, standardization bodies, and end-users is essential to ensure that these solutions are robust, scalable, and aligned with societal values.

In conclusion, the integration of blockchain and AI is not just an academic concept but a practical foundation for the next generation of cybersecurity solutions. With continued research and a commitment to responsible innovation, we can build intelligent, decentralized, and resilient infrastructures that empower secure digital transformation [10].

References

[1] M. Samaniego and R. Deters, "Blockchain as a Service for IoT," in *IEEE International Conference on Internet of Things (iThings)*, 2016, pp. 433–436. Available: https://ieeexplore.ieee.org/document/7879433

[2] M. A. Ferrag, L. Shu, X. Yang, A. Derhab, and L. Maglaras, "Security and Privacy for Green IoT-Based Agriculture: Review, Blockchain Solutions, and Challenges," *IEEE Access*, vol. 8, pp. 32031–32053, 2020. Available: https://ieeexplore.ieee.org/document/9017341

[3] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018. Available: https://www.sciencedirect.com/science/article/abs/pii/S0167739X17310191

[4] T. Salman and R. Jain, "A Survey of Protocols and Standards for Internet of Things," *Advanced Computing and Communications*, vol. 1, no. 1, pp. 1–14, 2019.

[5] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an Optimized Blockchain for IoT," in *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation*, 2017, pp. 173–178. Available: https://dl.acm.org/doi/10.1144/3054977.3055003

[6] Y. Lu, "The blockchain: State-of-the-art and research challenges," *Journal of Industrial Information Integration*, vol. 15, pp. 1–10, 2019. Available: https://doi.org/10.1016/j.jii.2019.100007

[7] J. Ni, K. Zhang, X. Lin, and X. Shen, "Securing Fog Computing for Internet of Things Applications: Challenges and Solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 601–628, 2018. Available: https://ieeexplore.ieee.org/document/8057280

[8] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[9] A. Sharma, R. Kaushal, and V. P. Singh, "A Survey on Intrusion Detection Systems and Techniques in Cloud," *Journal of Network and Computer Applications*, vol. 122, pp. 1–11, 2018. Available: https://www.sciencedirect.com/science/article/abs/pii/S1084804518302273

[10] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated Machine Learning: Concept and Applications," *ACM Transactions on Intelligent Systems and Technology (TIST)*, vol. 10, no. 2, pp. 1–19, 2019. Available: https://dl.acm.org/doi/10.1145/3298981

[11] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized Access Control with Anonymous Authentication for Securing Data in Clouds," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 384–394, 2014. Available: https://ieeexplore.ieee.org/document/6574875

[12] J. Konecny, H. B. McMahan, D. Ramage, and P. Richtarik, "Federated Optimization: Distributed Machine Learning for On-Device Intelligence," *arXiv preprint arXiv:1610.02527*, 2016. Available: https://arxiv.org/pdf/1610.02527

[13] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in *IEEE International Congress on Big Data*, 2017, pp. 557–564. Available: https://ieeexplore.ieee.org/document/8029300