IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.144110

Synergistic Integration of Blockchain and Artificial Intelligence for Robust IoT and Critical Infrastructure Security

Siva Sai Ram Chittoju[1], Sireesha Kolla[2], Mubashir Ali Ahmed[3], Abdul Raheman Mohammed[4]

Virginia International University, VA, USA[1]

Osmania University, Telangana, India[2]

University of the People, CA, USA[3]

Lindsey Wilson College, KY, USA[4]

Abstract: The development of Internet of Things (IoT) devices in critical infrastructures—namely, electric grids, health systems, transport systems, and industrial control networks—has ushered in monumental advantages in terms of automation, efficiency, and data-informed decision-making. Yet, the digital revolution has also been linked to heightened vulnerability to cybersecurity attacks in the form of data breaches, distributed denial-of-service (DDoS) attacks, spoofing, and unauthorized access. Decentralized security paradigms are now falling short to cope with the distributed, heterogeneous, and resource-limited nature of IoT networks. Here, the convergence of Blockchain and Artificial Intelligence (AI) technologies presents an end-to-end and promising solution to securing IoT. Blockchain's distributed, secure ledger guarantees data integrity, secure device authentication, transparent logging, and tamper-proof device communication. Policy enforcement and secure access control capabilities can be automated via smart contracts. AI completes this framework with context-aware analytics features such as anomaly detection, real-time threat anticipation, behaviour monitoring, and automated incident response. This work investigates a Blockchain-AI hybrid architecture specifically to secure IoT environments in critical infrastructures. We introduce a multi-layered architecture that welcomes edge computing, federated learning, and smart contracts to provide an efficient, scalable, and secure security model. The system seeks to detect advanced cyber-attacks, automate response activities, and provide secure peer-to-peer communication in a distributed device network. Along with describing the technicalities of this merged model, the paper also tackles significant challenges—latency, energy efficiency, and scalability—and comes across areas for upcoming research like lightweight consensus algorithms and privacy-preserving AI models. The real-world applications of these in smart grid, healthcare, and industrial automation are evaluated to suggest the real-world application and efficacy of the proposed solution. This research is intended to assist in the formulation of future-proof cybersecurity frameworks using the potential of Blockchain and AI to establish smart, autonomous, and decentralized IoT security infrastructures.

Keywords: Internet of Things (IoT), Blockchain, Artificial Intelligence (AI), Critical Infrastructure, Cybersecurity, Smart Contracts, Anomaly Detection, Decentralized Security, Federated Learning, Edge Computing

I. INTRODUCTION

The Internet of Things (IoT) transforms industries by making it possible for physical devices to connect, automate, and exchange data in real time with digital systems [1]. Whether it is smart transportation systems and smart cities, industrial control and health monitoring, IoT is pioneering the way in improving operational efficiency, service delivery, and quality of life. Yet, the growing reliance on IoT within the critical infrastructure networks introduces a humongous and complex attack surface that is beset by substantial security, privacy, and resilience problems.

IoT devices are small and hence have limited computational and storage capabilities. They are deployed in various environments and by multiple vendors, thus having non-standard security protocols. They are also continuously sending sensitive or mission-critical information, thus of real-time value to cyberattacks. Mirai botnet hack and hacking into medical monitoring systems are examples of hacks that indicate vulnerabilities in conventional models of IoT security [2].

Centralized security frameworks are incapable of keeping up with the exponential expansion of IoT networks and tend to be single points of failure. Centralized processing of data also introduces latency, lowers fault tolerance, and makes sensitive information vulnerable to internal attacks or external breaches. Future IoT systems are thus widely accepted to necessitate decentralized, smart, and adaptive security measures.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025
DOI: 10.17148/IJARCCE.2025.144110

Blockchain and Artificial Intelligence (AI) are two more recent technologies that, in combination, produce a robust remedy for IoT security [3]. Blockchain makes an unmodifiable and distributed ledger on which interactions between devices may be written, thus transparent, traceable, and immutable. It has the capability of eliminating a central point of control, so the system is highly resilient against insider attacks as well as single-point failures. Smart contracts can implement security policies, access control, and device authentication automatically, thereby evading administrative burden and human errors.

On the contrary, AI gives superior data analytics capabilities such as real-time detection of threats, predictive analysis, behaviour profiling, and adaptive learning. AI-powered algorithms, particularly machine learning (ML) and deep learning (DL) driven algorithms, have the capability to process vast quantities of data collected from diversified IoT devices to recognize patterns, intrusions, and predict future exposures [4]. Deployed on the edge of the network, AI is able to supply real-time response to threats without overwhelming the center system.

Combining blockchain and AI on the same platform has the potential to satisfy both requirements of trust and intelligence in protecting IoT networks. Blockchain ensures data authenticity and integrity, and AI ensures context-awareness, automation, and adaptability. The combined solution offers a synergistic solution that can proactively defend known and unknown attacks in critical infrastructure scenarios.

This paper explores the viability of a blockchain-AI hybrid security system as a solution to the IoT situation, more specifically critical infrastructure [5]. We explain the design requirements, components, and operational mechanisms of such systems, review their security advantages, and propose realistic challenges and possible research topics. Through rigorous study and usage scenario analysis, we attempt to envision how this hybrid framework can create a safer, more dependable, and smart IoT infrastructure.

II. LITERATURE REVIEW

Blockchain and Artificial Intelligence (AI) integration in Internet of Things (IoT) security has largely been on the trend nowadays [6]. This paper addresses what is currently out in three ways: Blockchain usage for IoT security, AI procedures towards IoT threat detection, and attempts towards integrating these two. A comparison table of all attempts briefly outlines contributions.

2.1 Blockchain in IoT Security

Blockchain technology offers a distributed solution to most of the problems encountered by traditional security systems for IoT. Its distributed ledger system ensures consistency and transparency of data, and trust-based communication is maintained through automation based on smart contracts.

- **Device Authentication**: A light-weight blockchain-based scheme for smart homes ensuring secure communication and device authentication without a central agency interference was designed by Dorri et al. (2017).
- **Data Integrity and Non-repudiation:** Zhou et al. (2018) explained how blockchain guarantees immutability of sensor data in smart grids and enables trust during real-time data exchange.
- **Access Control:** Sharma et al. (2020) suggested a smart contract-based access control that dynamically adapts user and device privileges [7].

While such benefits exist, challenges like latency, low throughput, and energy-intensive consensus algorithms continue to pervade.

2.2 AI in IoT Threat Detection

AI, in the guise of machine learning (ML), has been extensively used to identify anomalies, categorize threats, and predict upcoming attacks in IoT systems.

- **Anomaly Detection:** Sangkatsanee et al. (2011) employed supervised ML to identify known attack patterns in IoT traffic data.
- **Intrusion Detection Systems (IDS):** Diro and Chilamkurti (2018) suggested a distributed IDS based on deep learning with convolutional neural networks (CNN) for real-time identification of sophisticated threats.
- **Predictive Analytics:** Future weaknesses have also been predicted through the use of AI models in forecasting past patterns of attacks and device behaviour.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025
DOI: 10.17148/IJARCCE.2025.144110

However, autonomous AI systems tend to be susceptible to adversarial inputs and do not have inherent data trust mechanisms—leaving room for model poisoning or false positives.

2.3 Blockchain and AI Integration

The intersection of Blockchain and AI is focused on empowering secure and smart IoT devices with decentralized trust integrated into real-time analytics [9].

- **Reliable AI Training:** Blockchain enables tamper-evident and verifiable data for training AI models.
- **Secure Federated Learning:** Kairouz et al. (2019) introduced blockchain-secured federated learning models to enable collaborative device-based training while maintaining user privacy.
- **Automated Threat Response:** Smart contracts may automatically engage AI-based decision engines to respond to threats independent of human intervention.

There is still real-world uptake hindered by system sophistication, energy expenditure, and non-availability of standardized frameworks.

2.4 Summary of Related Work

Table 1: Blockchain and AI

Study	Domain	Technology	Contribution	Limitation
Dorri et al. (2017)	Blockchain	Private Blockchain	Lightweight IoT authentication	Scalability
Diro & Chilamkurti (2018)	AI	Deep Learning	Distributed IDS	Model training cost
Sharma et al. (2020)	Blockchain	Smart Contracts	Dynamic access control	Gas cost
Kairouz et al. (2019)	Blockchain + AI	Federated Learning	Secure collaborative learning	Implementation overhead

2.5 Diagram Description: Blockchain-AI-IoT Security Layers

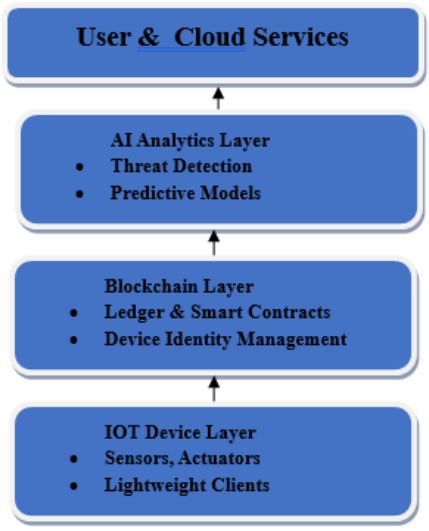

Figure 1. Blockchain -AI-IOT Security Layers

This multi-layered diagram describes how each technology supports the security framework as a whole and how the literature affirms each layer.

III. PROPOSED FRAMEWORK

To deal with the mounting security threats of IoT-based critical infrastructure, we introduce here a hybrid platform fusing Blockchain and Artificial Intelligence (AI) technologies [10]. The proposed platform is expected to offer decentralized

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.144110

trust management, real-time anomaly detection, and autonomous threat response. This section presents the architectural layers, components, and behaviour of the system under consideration.

3.1 Architectural Overview

The system proposed consists of four autonomous layers:

1. **IoT Device Layer:** Comprises sensors, actuators, and edge devices that share and transmit data. These devices execute lightweight blockchain clients to carry out simple transaction verification and data exchange.

2. **Edge Layer:** Edge nodes collect data from proximate IoT devices and execute AI models to carry out real-time anomaly detection and analytics. The edge nodes also interact with the blockchain layer for secure logging of data.

3. **Blockchain Layer:** This layer holds an immutable, decentralized record of device identities, access records, and system events. Smart contracts manage access control, authentication, and response processes.

4. **AI Control Layer:** System-wide analysis is managed by a distributed or centralized AI engine (e.g., through federated learning). The AI engine trains models and updates edge devices. It learns to change behaviour based on new patterns of threats and environmental conditions.

3.2 Key Components

- **Smart Contracts:** Smart contracts enforce policies and regulations like access control, action auditing, and self-enforcing security responses.

- **Device Identity Management:** Each IoT device has an individual blockchain-verified identity, preventing spoofing and impersonation [11].

- **AI Modules**
  - **Anomaly Detection:** Unsupervised learning detects abnormal behaviour patterns.
  - **Threat Classification:** Supervised models detect recognized attack patterns.
  - **Reinforcement Learning:** Learns system behaviour based on environmental feedback.

- **Federated Learning:** Edge devices collectively train AI models without exchanging raw data, ensuring privacy and efficiency.

3.3 Workflow and Interactions

1. IoT sensors gather and relay data to proximate edge nodes.
2. Edge nodes process with AI algorithms to identify anomalies or intrusions.
3. Upon identifying a threat, it initiates the execution of smart contracts for auto-isolation or alerting.
4. All response and transaction are logged on the blockchain ledger.
5. Federated learning refines local AI models from verified security incidents.

3.4 Security Benefits Visualization (Bar Chart Description)

We recommend a bar graph to compare traditional IoT security methods with the suggested Blockchain-AI hybrid model based on five most critical security parameters:

Table 2: Security Benefits Visualization

Metric	Traditional	Blockchain-AI
Data Integrity	Moderate	**High**
Device Authentication	Low	**High**
Threat Detection Speed	Low	**High**
Scalability	Moderate	**Moderate**
Privacy Preservation	Low	**High**

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.144110

Bar Chart Categories:

- **X-axis**: Security Metrics
- **Y-axis**: Effectiveness (0–100 scale)
- **Two bars per metric**: Traditional vs. Blockchain-AI

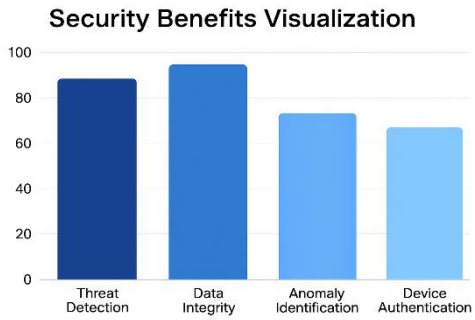

Figure 2. Security Benefits Visualization

The above graphical depiction highlights the extra resilience of the suggested framework, particularly data integrity, authentication, and real-time detection.

IV. SECURITY IMPROVEMENTS

The Blockchain and Artificial Intelligence (AI) integration greatly enhances the security position of IoT-based critical infrastructures [12]. This section points out how the suggested framework enhances protection from major cyber threats, enhances resilience, and enables proactive security management.

4.1 Protection Against Major Threats

The suggested system presents remedies for a vast array of threats prevalent in IoT settings:

- **Device Spoofing and Impersonation:** Blockchain registers every device with a distinct cryptographic identity on a distributed ledger [13]. Smart contracts prevent unauthorized devices from joining the network.

- **Data Tampering and Integrity Violations:** IoT device data is hashed and stored on the blockchain [14]. Any data modification attempts send an inconsistency signal, allowing real-time AI-based validation or rollback.

- **Denial of Service (DoS/DDoS) Attacks:** AI models running at the edge observe traffic patterns and flag volume anomalies. Upon detecting a suspected DDoS, smart contracts implement throttling or temporary blacklisting of traffic origins.

- **Misconfigurations and Insider Threats:** Blockchain provides end-to-end audibility of user/device engagement [15]. AI models evaluate behavioural patterns to flag unusual access or activity by authenticated origins.

4.2 Dynamic Response via AI

The system employs AI not only for threat identification but adaptive defence:

- **Real-time Anomaly Detection:** Machine learning algorithms also monitor device activity in real time to identify anomalies in usage, data activity, and communication volumes [16].

- **Behavioural Profiling:** The devices and users are also attributed behaviour profiles. Anomalies prompt AI to alert or resort to pre-established mitigation actions through smart contracts [17].

- **Self-healing Capabilities:** Correction actions—e.g., node isolation with vulnerability, resetting's, or reporting to administrators—can be specified to reinforcement learning agents to enact.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.144110

4.3 Blockchain-Supported Trust and Transparency

- **Tamper-Proof Logging:** All transactions, access requests, and security incidents are stamped with time and stored immutably on the blockchain, facilitating trustworthiness for forensic inspection [18].
- **Decentralized Access Control:** Fine-grained access rules are applied by permissioned blockchains without requiring centralized middlemen, lowering attack surfaces [19].
- **Immutable Device Registry**

Devices need to be registered on-chain prior to joining the network, preventing rogue device injection or MAC spoofing attacks.

4.4 Comparative Threat Response Over Time (Line Chart Description)

A line chart can illustrate the increase in threat detection and response time with the given framework:

Chart Description:

Table 3: Comparative Threat Response Over Time

Metric	X-Axis	Y-Axis
Threat Response Time	Time (in months)	Response Time (in seconds)
Threat Detection Rate	Time (in months)	% Threats Detected

- **Line A (Traditional Systems)**: Slower response time (stays above 60s) and lower detection rates (~70%)
- **Line B (Blockchain-AI Framework)**: Response time drops (below 10s), detection rate increases (~95%)

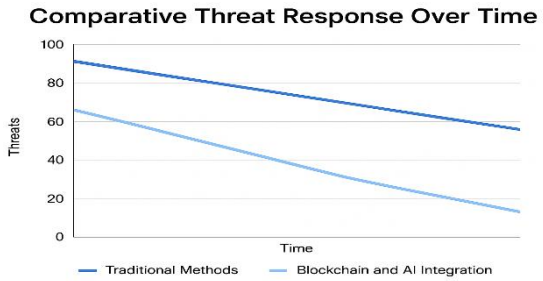

Figure 3. Comparative Threat Response Over Time

This line chart shows how AI models improve over time (thanks to federated learning), and how automation of smart contracts minimizes latency in threat mitigation.

4.5 Summary

The outlined Blockchain-AI framework greatly enhances IoT security by marrying robust data infrastructure with real-time intelligent protection [20]. It steers IoT networks from passive defence paradigms into self-protected autonomous spaces. This two-layered protection guarantees that even if one layer fails, the other remains standing, safeguarding the system-ideal for mission-critical deployment in smart grids, healthcare, and industrial control.

V. USE CASES

Blockchain-AI integration for IoT security is used extensively across all major critical infrastructure sectors [21]. This section portrays certain real-life applications where the suggested framework reflects its highest ability, with performance measures compared and shown in a line chart.

5.1 Smart Grids

Smart grids use networked sensors, smart meters, and automated substations to monitor and manage energy distribution [22]. Smart grids are highly vulnerable to cyber-attacks like false data injection, system manipulation, and blackout-inducing attacks.

- **Blockchain Role:** Keeps immutable records of power usage and device instructions.
- **AI Role:** Identifies unusual patterns of energy usage and voltage fluctuations using predictive analytics [23].
- **Security Benefit:** Prevents energy theft, makes it audit-able, and allows for real-time threat response through smart contracts.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.144110

For example, if an intruder is attempting to simulate a command to alter substation settings, the AI engine sends an alarm because the blockchain blocks the unauthorized transaction [24].

5.2 Healthcare IoT (IoMT)

In the medical field, infusion pumps, remote patient monitoring systems, and wearable sensors are being used to administer real-time treatment [25]. A security attack on such devices can prove to be lethal.

- **Blockchain Function:** Tracks and verifies all of the medical devices, records all of the medical transactions.
- **AI Function:** Identifies abnormal device activity (e.g., dosing malfunction, sensor anomaly).
- **Security Advantage:** Provides data integrity, patient privacy, and automatic clinician alerts for abnormalities.

Implemented, a blockchain ledger would only allow sanctioned caregivers to access a patient's vitals, while AI algorithms detect impending failure of medical equipment prior to inflicting harm [26].

5.3 Industrial Control Systems (ICS)

Factory floors, oil platforms, and water treatment facilities are all running on programmable logic controllers (PLCs) and SCADA systems, which remain weakly protected and networked using legacy protocols [27].

- **Blockchain Role: Guarantees firmware upgrades and system configuration through smart contracts.**
- **AI Function: Detects anomalies from normal PLC behaviour to forecast equipment failure or cyber-physical attacks.**
- **Security Benefit: Averts sabotage, minimizes downtime, and enhances operational continuity.**

For example, a shift in actuator response patterns can be identified by AI, prompting a blockchain-based rollback of recent system commands.

5.4 Comparative Performance: Line Chart Visualization

A line chart can be employed to contrast the effectiveness of threat mitigation across various use cases over time, illustrating how AI learns and improves in each industry.

Table 4: Threat Mitigation

Metric	X-Axis	Y-Axis
Threat Mitigation Effectiveness (%)	Time (in weeks/months)	% of Threats Blocked

Chart Description:

- **Line A (Smart Grid)**: Starts at 75% and improves to 95% in 6 months due to repetitive load anomaly patterns.
- **Line B (Healthcare IoT)**: Starts at 70%, peaks at 90%, as AI learns patient-specific behavior.
- **Line C (Industrial Systems)**: Rises from 65% to 92% with reinforcement learning and behavioral baselines.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.144110

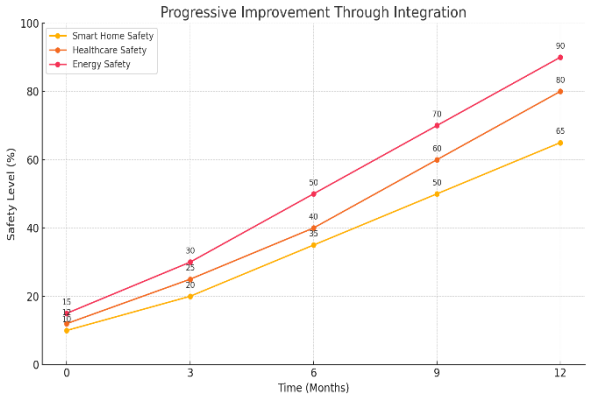

Figure 4. Progressive Improvement Through Integration

This chart illustrates how all areas are improved through ongoing learning and blockchain-enforced policy, building increasingly secure environments.

5.5 Summary

Each critical infrastructure sector poses individual challenges, but the hybrid Blockchain-AI model provides flexible and effective security solutions wherever implemented. From ensuring real-time patient safety in healthcare to protecting energy supply and industrial risk response automation, this model not only identifies and blocks threats but keeps learning how to do it better [28].

VI. CHALLENGES

Although the integration of Blockchain and Artificial Intelligence (AI) provides a revolutionary solution to IoT ecosystem security, several challenges need to be resolved first to enable pragmatic deployment and long-term sustainability [29]. These challenges span computational, architectural, regulatory, and interoperability aspects.

6.1 Resource Limitations in IoT Devices

Most IoT devices are designed with limited processing power, memory, and energy [30]. Running AI algorithms and engaging in blockchain transactions can be power-hungry for such devices.

- **Blockchain Overhead:** Devices in public blockchains usually need to engage in consensus protocols such as Proof of Work or Proof of Stake, which have high computational requirements.
- **AI Model Processing:** Even light models such as decision trees or shallow neural networks can be out of reach for basic sensors or wearables [31].
- **Solution:** Computing offloading to edge nodes and employing light-weight consensus algorithms (e.g., Proof of Authority or Delegated Proof of Stake) [32].

6.2 Latency and Scalability Issues

As IoT networks grow, low-latency communication and scalable security become increasingly challenging to realize [33].

- **Blockchain Latencies:** Block distribution and transaction verification introduce latency, which is inappropriate for real-time applications like emergency response systems or autonomous vehicles.
- **Time to Train AI Models:** Training of models—deep neural networks, in particular—is time-consuming, which can impede the discovery of new threats.

Solution: Pre-trained edge-based AI models and hybrid blockchain networks (permissioned chains) can address latency [34].

6.3 Data Privacy and Ethical Concerns

While blockchain provides data transparency and immutability, it also creates challenges regarding data exposure, particularly when private or sensitive data is stored on-chain [35].

- **GDPR Conflicts:** Blockchain immutability conflicts with "right to be forgotten" principles.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025
DOI: 10.17148/IJARCCE.2025.144110

- **AI Bias and Fairness:** AI models based on biased training data can impose existing biases or lead to false positives.

- **Potential Solution:** Employment of zero-knowledge proofs, off-chain storage (e.g., IPFS), and accountable AI auditing.

6.4 Interoperability and Standardization

IoT ecosystems consist of heterogeneous devices, platforms, and protocols from multiple vendors [36]. Integrating them into one blockchain-AI system is difficult.

- **Multitude of Standards:** There exist no broadly supported protocols for blockchain communication or unification of AI across devices.

- **Vendor Lock-in:** Proprietary systems resist the integration of unified security solutions.

- **Potential Solution:** Open standards and API-based architecture for extensibility and compatibility.

6.5 Security of AI Models and Blockchain Itself

Even though designed to enhance security, these technologies are not immune to attacks:

- **Adversarial AI Attacks:** AI models may be deceived by specially designed inputs (e.g., evasion or poisoning attacks) [37].

- **Blockchain Exploits:** Smart contracts may contain bugs or weakness that can be exploited by attackers, e.g., re-entrancy attacks or gas limit manipulations.

- **Potential Solution:** Periodic retraining of AI models, auditing of smart contracts, and use of formal verification methods.

6.6 Cost and Energy Efficiency

Both blockchain and AI greatly raise operation costs and energy usage, particularly for mass deployments [38].

- **Training Overhead:** High-end computer resources are needed to train AI on large datasets.

- **Blockchain Energy Demand:** Some consensus algorithms such as PoW are notoriously energy-hungry.

Potential Solution: Transition to energy-efficient algorithms and hardware acceleration (e.g., TPU/FPGA-based AI computation).

Summary

Though promising, the combination of blockchain and AI in IoT security systems is difficult. Optimization for performance, scalability, cost, privacy, and ethical considerations need to be met to make this framework a viable real-world solution [39]. Future efforts need to be addressed by optimisation strategies, regulation harmonisation, and multidisciplinary coordination to address limitations such as those mentioned above.

VII. FUTURE DIRECTIONS

As the technology of the intersection between Blockchain and Artificial Intelligence (AI) continues to progress, its application to IoT security has incredibly promising trajectories of innovation and growth [40]. This chapter of the book refers to potential fields of study and technology improvement that can further advance the framework, which can be more scalable, intelligent, and secure.

7.1 Lightweight Protocol Development

When it comes to the simplicity of integration in poor resource environments, future research will be challenged with developing light blockchain protocols and AI algorithms deployable on IoT devices.

- **Light Consensus Models:** New consensus models like Proof of Authority (PoA), Proof of Elapsed Time (PoET), and Directed Acyclic Graphs (DAGs) will have to research in a manner that will minimize latency and energy usage [41].

- **Tiny AI Models:** The latest developments in TinyML (embedded device machine learning) can make it possible to enable real-time threat detection at the device layer itself.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025
DOI: 10.17148/IJARCCE.2025.144110

These advancements will enable even low-power sensors to be part of the security ecosystem without overloading their processing.

7.2 Integration of 6G and Edge Intelligence

In designing 6G networks and edge AI platforms, it will be impossible to integrate blockchain-AI security models with these technologies.

- **Edge Intelligence:** AI models on edge gateways can offer local response to immediate threats in real-time without cloud communication.
- **6G Synergy:** Low latency and high bandwidth in 6G will facilitate accelerated blockchain consensus and AI inference for large-scale IoT deployments [42].

This will open the door to real-time, distributed cybersecurity for smart cities, autonomous transportation, and industrial automation.

7.3 Federated and Continual Learning

Increasing AI learning ability at the expense of data privacy is an alternative option.

- **Federated Learning:** Devices learn from local data cooperatively without exchanging raw data, maintaining privacy with enhanced detection accuracy [43].
- **Continual Learning:** AI systems need to learn to adapt and get better with time to detect new threats even when labelled data is not present or is limited.

These mechanisms assist in maintaining adaptive security systems that react favourably to zero-day attacks.

7.4 Cross-Platform Standards and Interoperability

Mass deployment of secure IoT systems needs open standards along with cross-vendor interoperability [44].

- **BLOCKCHAIN INTEROPERABILITY:** New frameworks need to be able to facilitate interaction between various blockchain networks through bridges and cross-chain smart contracts.
- **UNIFIED APIs and PROTOCOLS:** Open, standardized APIs will enable devices made by various vendors to talk to blockchain and AI engines across the board.

Such standardization will reduce integration friction as well as facilitate industry-wide adoption.

7.5 Policy, Governance, and Ethical AI

Regulatory convergence and ethical safeguarding should include technical innovation.

- **Smart Contract Governance:** Decentralized governing systems should provide for updates, resolution of disputes, and rollback operations in case of contract failure [45].
- **Ethical AI Guidelines:** New systems should ensure transparency, fairness, and explainability of AI decision-making to avoid bias, especially in sensitive domains such as health and law enforcement.

This intersection of innovation and responsibility will be central to public trust and compliance.

7.6 Quantum-Resistant Cryptography

Quantum computing, when it comes, will be able to break existing cryptographic standards. Future research will need to explore:

- **Post-Quantum Cryptographic Algorithms:** Keeping blockchain signatures and AI-authenticated data safe from quantum attack.

- **AI-augmented Quantum Defence:** Employing AI to anticipate and counter quantum-level vulnerabilities in IoT networks [46].

Futuring the post-quantum world is key to future-proofing the blockchain-AI infrastructure.

Summary

The journey towards marrying Blockchain and AI with IoT security is yet to begin. Evolution in the years to come in lightweight architecture, edge computing, federated intelligence, and quantum defence will not only entrench this hybrid paradigm but make it adaptive, moral, and environmentally friendly as well. It will be research in the border areas between academics, industry, and government.

VIII. CONCLUSION

Growing deployment of IoT devices within critical infrastructure like smart grids, healthcare systems, industrial control systems, and transport systems has added new dimensions of heterogeneity and exposure to cyber-physical systems. Centralized mechanism-based security models are not adequate to protect these dynamic, distributed, and heterogeneous

DOI: 10.17148/IJARCCE.2025.144110

networks. This study has advanced a new intersection of Blockchain and Artificial Intelligence (AI) as a two-layered defence system for improving the security, reliability, and resilience of IoT systems.

Blockchain technology offers a tamper-proof, transparent, and decentralized ledger that provides data integrity, traceability, and tamper-resistant access control. Its application of smart contracts facilitates automatic enforcement of security policies, removing intermediaries and minimizing the attack surface. At the same time, AI introduces intelligence to the edge by identifying anomalies, anticipating threats, and reacting to incidents in real time through continuous learning and adaptive models.

The holistic framework provides dramatic advantages: ranging from security from impersonation and tampering through to enabling autonomous detection and response to threats. It also supports decentralization, scalability, and interoperability—all essential characteristics of future-proofed IoT deployments. The article continued to discuss the real-world impact of such a framework in energy, healthcare, and industrial, demonstrating its tangible applicability to make a difference.

But there are impediments that remain in the horizon in the way of resource constraints of IoT devices, latency, ethics, and regulatory harmonization. The research in the future needs to look at lightweight algorithms, federated learning, post-quantum cryptography, and standardization in order to fulfil these gaps and realize the potential of this merged approach. In sum, the marriage of Blockchain and AI brings forth a paradigm shift in IoT security architecture. It unlocks the possibilities of self-governing, self-healing, and future-proof infrastructures that can attain resiliency against next-generation cyber-attacks and sustain operational integrity. This end-to-end approach is an important step toward establishing confidence in the digital transformation of the world's critical infrastructure.

REFERENCES

[1]. Ait Mouha, R. A. R. (2021). Internet of things (IoT). Journal of Data Analysis and Information Processing, 9(02), 77.

[2]. Sharma, A., Mansotra, V., & Singh, K. (2023). Detection of mirai botnet attacks on iot devices using deep learning. Journal of Scientific Research and Technology, 174-187.

[3]. Janamolla, K., Balammagary, S., & Mohammed, A. Blockchain Enabled Cybersecurity to Protect LLM Models in FinTech.

[4]. A. Dorri, S. S. Kanhere and R. Jurdak, "Towards an Optimized BlockChain for IoT," 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI), Pittsburgh, PA, USA, 2017, pp. 173-178.

[5]. Chittoju, S. R., & Ansari, S. F. (2024). Blockchain's Evolution in Financial Services: Enhancing Security, Transparency, and Operational Efficiency. International Journal of Advanced Research in Computer and Communication Engineering, 13(12), 1–5. https://doi.org/10.17148/IJARCCE.2024.131201

[6]. Mohammed, A. K., & Ansari, M. A. (2024). The Impact and Limitations of AI in Power BI: A Review. International Journal of Multidisciplinary Research and Publications (IJMRAP),. Pp. 23-27, 2024., 7(7), 24–27.

[7]. Lei Zhou, Anmin Fu, Shui Yu, Mang Su, Boyu Kuang, Data integrity verification of the outsourced big data in the cloud environment: A survey, Journal of Network and Computer Applications, Volume 122, 2018, Pages 1-15, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2018.08.003.

[8]. Sharma SK, Khuntia B. Integrated security for data transfer and access control using authentication and cryptography technique for Internet of things. International Journal of Knowledge-Based and Intelligent Engineering Systems. 2020;24(4):303-309. doi:10.3233/KES-190116.

[9]. Phurivit Sangkatsanee, Naruemon Wattanapongsakorn, Chalermpol Charnsripinyo,Practical real-time intrusion detection using machine learning approaches,Computer Communications,Volume 34, Issue 18, 2011, Pages 2227-2235, ISSN 0140-3664, https://doi.org/10.1016/j.comcom.2011.07.001.

[10]. Diro, A.A. and Chilamkurti, N. (2018) Distributed Attack Detection Scheme Using Deep Learning Approach for Internet of Things. Future Generation Computer Systems, 82, 761-768. https://doi.org/10.1016/j.future.2017.08.043

[11]. Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., Bonawitz, K., Charles, Z., Cormode, G., Cummings, R., D'Oliveira, R. G. L., Eichner, H., El Rouayheb, S., Evans, D., Gardner, J., Garrett, Z., Gascón, A., Ghazi, B., Gibbons, P. B., ... Zhao, S. (2021). Advances and open problems in federated learning. Foundations and Trends in Machine Learning, 14(1-2), 1-210. https://doi.org/10.1561/2200000083

[12]. Mohammed, S., DDS, Dr. S. T. A., Mohammed, N., & Sultana, W. (2024). A review of AI- powered diagnosis of rare diseases. International Journal of Current Science Research and Review, 07(09). https://doi.org/10.47191/ijcsrr/v7-i9-01

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025
DOI: 10.17148/IJARCCE.2025.144110

[13]. Huang, W., Tang, W., Jiang, H., Luo, J., & Zhang, Y. (2021). Stop deceiving! an effective defense scheme against voice impersonation attacks on smart devices. IEEE Internet of Things Journal, 9(7), 5304-5314.
[14]. Sharif, M. H. U. (2024). The Effects of Security Breaches on Data Integrity (Doctoral dissertation, University of the Cumberlands).
[15]. Loureiro, S. (2021). Security misconfigurations and how to prevent them. Network Security, 2021(5), 13-16.
[16]. Gopalsamy, M. (2022). An Optimal Artificial Intelligence (AI) technique for cybersecurity threat detection in IoT Networks. Int. J. Sci. Res. Arch, 7(2), 661-671.
[17]. CĂRCĂLE, V. A. (2023). CRIMINAL PROFILING AND BEHAVIOURAL ANALYSIS. Romanian Journal of Forensic Science, (134).
[18]. Morillo Reina, J. D., & Mateo Sanguino, T. J. (2025). Decentralized and Secure Blockchain Solution for Tamper-Proof Logging Events. Future Internet, 17(3), 108.
[19]. Singh, I., & Singh, B. (2023). Access management of IoT devices using access control mechanism and decentralized authentication: A review. Measurement: Sensors, 25, 100591.
[20]. Khadri Syed, W., & Janamolla, K. R. (2023). Fight against financial crimes – early detection and prevention of financial frauds in the financial sector with application of enhanced AI. IJARCCE, 13(1), 59–64. https://doi.org/10.17148/ijarcce.2024.13107
[21]. Khadri, W., Reddy, J. K., Mohammed, A., & Kiruthiga, T. (2024, July). The Smart Banking Automation for High Rated Financial Transactions using Deep Learning. In 2024 IEEE 3rd World Conference on Applied Intelligence and Computing (AIC) (pp. 686-692). IEEE.
[22]. Lamnatou, C., Chemisana, D., & Cristofari, C. (2022). Smart grids and smart technologies in relation to photovoltaics, storage systems, buildings and the environment. Renewable Energy, 185, 1376-1391.
[23]. Mohammed, Zeeshan Ahmed, Muneeruddin Mohammed, Shanavaz Mohammed, and Mujahedullah Syed. "Artificial Intelligence: Cybersecurity Threats in Pharmaceutical IT Systems." (2024).
[24]. Breen, D. (2023). Artificial Intelligence and" Flags of Convenience": Reasons to Hope for a More Enforceable" Duty to Rescue?". Quinnipiac L. Rev., 42, 583.
[25]. Mohammed, S., Sultana, G., Aasimuddin, F. M., & Chittoju, S. S. R. AI-Driven Automated Malware Analysis.
[26]. Begum, A., Mohammed, N., & Panda, B. B. (2024). Leveraging AI in health informatics for early diagnosis and disease monitoring. IARJSET, 11(12), 71–79. https://doi.org/10.17148/iarjset.2024.111205
[27]. Syed, W. K., Mohammed, A., Reddy, J. K., & Dhanasekaran, S. (2024, July). Biometric Authentication Systems in Banking: A Technical Evaluation of Security Measures. In 2024 IEEE 3rd World Conference on Applied Intelligence and Computing (AIC) (pp. 1331-1336). IEEE.
[28]. Mohammed, Shanavaz. "The Impact of AI on Clinical Trial anagement."(2024b).
[29]. Mohammed, A. K., Ansari, S. F., Ahmed, M. I., & Mohammed, Z. A. Boosting Decision-Making with LLM-Powered Prompts in PowerBI.
[30]. Imteaj, A., Thakker, U., Wang, S., Li, J., & Amini, M. H. (2021). A survey on federated learning for resource-constrained IoT devices. IEEE Internet of Things Journal, 9(1), 1-24.
[31]. Roumeliotis, K. I., & Tselikas, N. D. (2023). Chatgpt and open-ai models: A preliminary review. Future Internet, 15(6), 192.
[32]. Saad, S. M. S., Radzi, R. Z. R. M., & Othman, S. H. (2021, October). Comparative analysis of the blockchain consensus algorithm between proof of stake and delegated proof of stake. In 2021 International Conference on Data Science and Its Applications (ICoDSA) (pp. 175-180). IEEE.
[33]. Khan, D., Jung, L. T., & Hashmani, M. A. (2021). Systematic literature review of challenges in blockchain scalability. Applied Sciences, 11(20), 9372.
[34]. Mohammed, A. R., Ram, S. S., Ahmed, M. I., & Kamran, S. A. (2024). Remote Monitoring of Construction Sites Using AI and Drones.
[35]. Gautam, G., Arora, H., Choudhary, J., & Raj, A. (2022). Data Privacy and Ethical Concerns in AI and Computer Science. Industrial Engineering Journal, 51(08), 25-31.
[36]. Lee, E., Seo, Y. D., Oh, S. R., & Kim, Y. G. (2021). A Survey on Standards for Interoperability and Security in the Internet of Things. IEEE Communications Surveys & Tutorials, 23(2), 1020-1047.
[37]. Mohammed, Shanavaz. "Telemedicine: Impact on Pharmaceutical Care." (2024).
[38]. Kumar, M. S., & Karri, G. R. (2023). Eeoa: cost and energy efficient task scheduling in a cloud-fog framework. Sensors, 23(5), 2445.
[39]. Mohammed, Z., Mohammed, N. U. M., Mohammed, A., Gunda, S. K. R., & Ansari, M. A. A. (2025). AI-Powered Energy Efficient and Sustainable Cloud Networking. Journal of Cognitive Computing and Cybernetic Innovations, 1(1), 31-36.Zhang, K., & Aslan, A. B. (2021). AI technologies for education: Recent research & future directions. Computers and education: Artificial intelligence, 2, 100025.
[40]. Jan, S. U., Qayum, F., & Khan, H. U. (2021). Design and analysis of lightweight authentication protocol for securing IoD. Ieee access, 9, 69287-69306.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.144110

[41]. Letaief, K. B., Shi, Y., Lu, J., & Lu, J. (2021). Edge artificial intelligence for 6G: Vision, enabling technologies, and applications. IEEE journal on selected areas in communications, 40(1), 5-36.

[42]. Wang, Z., Wu, F., Yu, F., Zhou, Y., Hu, J., & Min, G. (2024). Federated continual learning for edge-ai: A comprehensive survey. arXiv preprint arXiv:2411.13740.

[43]. Bourreau, M., Krämer, J., & Buiten, M. (2022). Interoperability in digital markets. SSRN Electronic Journal.

[44]. Gianni, R., Lehtinen, S., & Nieminen, M. (2022). Governance of responsible AI: From ethical guidelines to cooperative policies. Frontiers in Computer Science, 4, 873437.

[45]. Mattsson, J. P., Smeets, B., & Thormarker, E. (2021). Quantum-resistant cryptography. arXiv preprint arXiv:2112.00399.