Publisher
Singh Publication
www.singhpublication.com

E-ISSN:2583-2468

Applied Science and Engineering Journal for Advanced Research

2025 Volume 4 Number 6 November

Research Article

Artificial Intelligence

# Blockchain and AI Amalgamation for IoT Applications beyond 5G: A Case Study of Enhancing Data Security and Privacy in 5G-IoT Ecosystems

**Bora MS[1*], Tewari P[2]**

DOI:10.5281/zenodo.18042753

[1*] Mahendra Singh Bora, Associate Professor, Department of Computer Science, Shriram Institute of Management and Technology, Kashipur, Uttarakhand, India.

[2] Pankaj Tewari, Assistant Professor, Department of Computer Science, Shriram Institute of Management and Technology, Kashipur, Uttarakhand, India.

The Internet of Things (IoT) in connection with blockchain technology and artificial intelligence (AI) concerning beyond 5G (B5G) networks promises a revolutionary means of coping with the most topical issues of data privacy and existing security concerns. With 5G technology indicating a new age of a higher connectivity, high bandwidth and ultra-low latency, it will also result in increasing the vulnerabilities that have been alleged with IoT ecosystems. In this research paper, we address the issue of how blockchain and AI can be integrated to enhance data security, data privacy within the 5G-IOT systems. The main directions are the use of the decentralized and immutable ledger with blockchain to securely conduct data transactions, applying the AI to intelligent processing of the data and real-time threats detection, the combination of the technologies to build robust, autonomous, and safe IoT systems.

**Keywords:** smart contracts, artificial intelligence, IoT, 5G, data security, privacy, 5G-IoT ecosystems

**Corresponding Author**

Mahendra Singh Bora, Associate Professor, Department of Computer Science, Shriram Institute of Management and Technology, Kashipur, Uttarakhand, India.
Email: mahendra.singh.bora@gmail.com

**How to Cite this Article**

Bora MS, Tewari P, Blockchain and AI Amalgamation for IoT Applications beyond 5G: A Case Study of Enhancing Data Security and Privacy in 5G-IoT Ecosystems. Appl Sci Eng J Adv Res. 2025;4(6):1-8. Available From https://asejar.singhpublication.com/index.php/ojs/article/view/174

**To Browse**

| Manuscript Received | Review Round 1 | Review Round 2 | Review Round 3 | Accepted |
|---|---|---|---|---|
| 2025-10-03 | 2025-10-22 | | | 2025-11-11 |

| Conflict of Interest | Funding | Ethical Approval | Plagiarism X-checker | Note |
|---|---|---|---|---|
| None | Nil | Yes | 6.79 | |

# 1. Introduction

Internet of Things (IoT) has revolutionized different industries through the ability of smart gadgets to communicate and trade information. The introduction of 5G networks enables the IoT applications to reach new measures of performance and efficiency. Yet, with the propagation of the connected devices and information exchange, there arises a set of challenges that is associated with security and privacy. This paper explores the potential of Blockchain and AI combination to deal with these issues which could securing information across 5G-IoT ecosystems.

### 1.1.1 5G Technology and IoT

The 5G technology is faster, has less latency, and has more connectivity that make it suitable to automation/IoT. It favours massive machine-type communications and ultra-reliable low latency communications, which are essential to different IoT applications.

### 1.1.2 Security and Privacy Challenges in 5G-IoT

Part of the 5G vulnerabilities is the presence of attack surface, advanced cyber threats and privacy issues alongside the 5G good things. The current security systems fail to meet these needs and newer solutions are required.

### 1.2.1 Overview of Blockchain

Blockchain is an open distributed ledger, transparent, and immutable technology that is protected by cryptographic hashing and consensus. It is much appropriate to secure IoT environment owing to its decentralized implication.

### 1.2.2 Blockchain for IoT Security

Blockchain may also be used to increase IoT security through ensuring a history of transactions that is tamper-proof and also secure peer-to-peer communication. It also helps to do away with centralized control and hence there is reduced risk of single points of failure.

### 1.3.1 Overview of AI

Artificial Intelligence (AI) is the acquisition of algorithms and systems that can undertake tasks that need human intelligence. Within the realm of the IoT, AI has the capability of sifting through large scale data, identifying anomalies, and real-time decision-making.

### 1.3.2 AI for IoT Security

AI can secure IoT by detecting patterns, anticipating and responding to potential threats, and automating responses. Machine learning algorithms, such as, can learn over time from the data to be continually improving your security.

### 1.4 Amalgamation of Blockchain and AI

### 1.4.1 Synergistic Benefits

The problem is that the combination of Blockchain and AI presents synergistic advantages when improving the IoT security. The use of blockchain along with AI yields a dynamic security network that cannot be easily hacked and is transparent in its operation.

### 1.4.2 Framework for Integration

The proposed framework involves using Blockchain for secure data storage and transaction validation, while AI is employed for data analysis, threat detection, and automated response. Smart contracts on the Blockchain can automate processes based on AI-driven insights.

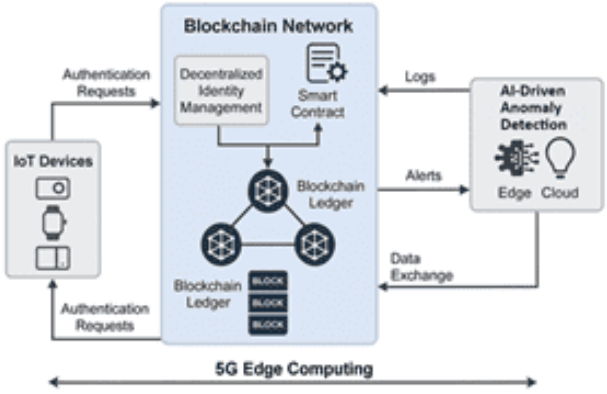


**Figure 1:** Proposed blockchain–AI security architecture for 5G-enabled IoT edge computing. The framework integrates decentralized authentication, smart contract-based access control, and AI driven anomaly detection to mitigate security threats. It supports real-time transaction logging and adaptive policy enforcement across permissioned blockchain networks. [16]

# 2. Application Areas of IoT

IoT has many applications in many fields of industry, based on the benefits of remote controlling

and managing connected devices, gathering and processing data in real-time, and having device-related processes automated. Listed below are some of the major areas of applications of IoT:

**1. Smart Cities**

IoT technology is transforming urban areas into smart cities, enhancing the quality of life for residents and improving city management.

***Smart Infrastructure:*** Monitoring and managing infrastructure such as bridges, roads, and buildings for maintenance and safety.

***Smart Lighting:*** Implementing intelligent lighting systems that adjust based on occupancy and daylight, reducing energy consumption.

***Smart Waste Management:*** Optimizing waste collection routes and schedules using sensors in waste bins.

**2. Healthcare**

IoT is revolutionizing healthcare by enabling remote monitoring, personalized treatment, and efficient management of healthcare facilities.

***Remote Patient Monitoring:*** Wearable devices and sensors track vital signs and health metrics, allowing for real-time monitoring by healthcare providers.

***Smart Medical Devices:*** Connected medical devices that provide real-time data to clinicians, improving diagnosis and treatment.

***Telemedicine:*** Facilitating virtual consultations and remote healthcare services.

**3. Industrial IoT (IIoT)**

IoT in the industrial sector is used to promote automation, predictive maintenance as well as operational effectiveness.

***Predictive Maintenance:*** Sensors monitor equipment conditions to predict failures and schedule maintenance before breakdowns occur.

***Supply Chain Management:*** Enhancing visibility and efficiency in logistics and inventory management through real-time tracking.

***Smart Manufacturing:*** Using IoT to optimize production processes, monitor equipment performance, and ensure quality control.

**4. Agriculture**

IoT will make possible precision agriculture, increase crop yield, and better use resources.

***Smart Irrigation Systems:*** Automated irrigation according to the level of soil moisture and weather conditions.

***Livestock Monitoring:*** Tracking the health and location of livestock using wearable devices.

***Crop Monitoring:*** Using sensors and drones to monitor crop health, soil conditions, and environmental factors.

**5. Smart Homes**

IoT technology is enhancing home automation, security, and energy management.

***Home Automation:*** Controlling lighting, heating, cooling, and appliances through smart devices and apps.

***Home Security Systems:*** Smart cameras, doorbells, and locks providing real-time surveillance and alerts.

***Energy Management:*** Monitoring and optimizing energy consumption through smart meters and connected devices.

**6. Retail**

IoT is changing retail customer experience by handling stocks, understanding customers, and personalized shopping.

***Smart Shelves:*** Sensors that track inventory levels and trigger automatic restocking.

***Customer Insights:*** Collecting data on customer behaviour and preferences to offer personalized experiences.

***Automated Checkouts:*** Reducing wait times and enhancing convenience with IoT-enabled checkout systems.

**7. Transportation and Logistics**

IoT enhances transportation systems, improves logistics efficiency, and ensures safety.

***Fleet Management:*** Real-time tracking and management of vehicle fleets to optimize routes and reduce fuel consumption.

***Smart Traffic Management:*** Using sensors and data analytics to manage traffic flow and reduce congestion.

***Connected Vehicles:*** Enabling vehicle-to-vehicle and vehicle-to-infrastructure communication for improved safety and autonomous driving.

**8. Energy Management**

IoT is playing a critical role in optimizing energy production, distribution, and consumption.

***Smart Grids:*** Enhancing the efficiency and reliability of electricity distribution networks.

***Renewable Energy Management:*** Monitoring and managing renewable energy sources like solar and wind.

***Energy Consumption Monitoring:*** Using smart meters and sensors to track and optimize energy usage in homes and businesses.

**9. Environmental Monitoring**

IoT devices are used for monitoring environmental conditions and addressing ecological challenges.

***Air Quality Monitoring:*** Sensors that track pollution levels and provide real-time data to inform public health decisions.

***Water Quality Monitoring:*** IoT devices that monitor water bodies for contaminants and ensure safe drinking water.

***Wildlife Conservation:*** Tracking the movement and health of wildlife to support conservation efforts.

**10. Smart Wearables**

Wearable IoT gadgets can be used to improve personal health, fitness, and lifestyle control.

***Fitness Trackers:*** Devices that monitor physical activity, heart rate, sleep patterns, and other health metrics.

***Smart Watches:*** Wearables that offer health tracking, notifications, and connectivity with other devices.

***Medical Wearables:*** Devices that monitor chronic conditions, such as glucose monitors for diabetes management.

# 3. Sources of Security Threats In IoT Applications

The security threats that IoT applications are subjected to are diverse because they are connected to each other and traverse with a lot of data. Principal vulnerabilities of IoT applications stemming off security threats are:

**1. Device-Level Threats**

**a. Insecure Devices**

***Poorly Configured Devices:*** Many IoT devices are shipped with default settings that are not secure, such as default passwords.

***Unpatched Vulnerabilities:*** Devices often run outdated firmware or software with known vulnerabilities that are not updated or patched.

**b. Physical Attacks**

***Tampering:*** Physical access to devices can allow attackers to alter hardware or firmware.

***Side-Channel Attacks:*** Techniques such as power analysis or electromagnetic analysis can be used to extract sensitive information.

**2. Network-Level Threats**

**a. Eavesdropping**

***Data Interception:*** Unencrypted data transmitted between devices and servers can be intercepted and read by unauthorized parties.

**b. Man-in-the-Middle (MitM) Attacks**

***Session Hijacking:*** Attackers intercept and potentially alter communication between IoT devices and their controlling applications.

**c. Denial of Service (DoS) Attacks**

***Network Flooding:*** Overwhelming IoT devices or networks with traffic to disrupt services.

**3. Application-Level Threats**

**a. Insecure Interfaces**

***APIs and Web Interfaces:*** Vulnerable APIs and web interfaces can be exploited to gain unauthorized access or control over IoT devices.

***Weak Authentication and Authorization:*** Insufficient mechanisms to ensure that only authorized users and applications can access and control IoT devices.

**b. Malware**

***IoT-Specific Malware:*** Malicious software designed to exploit vulnerabilities in IoT devices for purposes such as data theft, botnet creation, or ransomware.

**4. Data-Level Threats**

**a. Data Breaches**

***Unauthorized Access:*** Sensitive data stored on IoT devices or transmitted across networks can be accessed by unauthorized entities.

***Insufficient Encryption:*** Lack of encryption or weak encryption algorithms can lead to data being compromised.

**b. Data Integrity Attacks**

***Data Tampering:*** Attackers alter data being transmitted or stored, leading to incorrect information being processed and acted upon.

**5. Supply Chain Threats**

**a. Hardware Compromise**

***Malicious Components:*** The manufacturing process of adding malicious components or backdoors into the manufacturing process.

***Counterfeit Devices:*** Use of counterfeit devices that have vulnerabilities or malicious capabilities embedded.

**b. Software Supply Chain Attacks**

***Compromised Software:*** Malicious code introduced into software or firmware updates provided by third-party vendors.

**6. Human Factors**

**a. Insider Threats**

***Disgruntled Employees:*** Having access to the IoT systems, employees can abuse their privileges and steal data or cause disruption of operations.

***Unintentional Errors:*** Human failure/mistake like wrong device configuration, mishandling of devices or being caught in a phishing attack.

**b. Social Engineering**

***Phishing:*** Attackers tricking users into providing sensitive information or access credentials.

***Pretexting:*** Deceiving users into performing actions that compromise security by pretending to be someone they trust.

**7. Systemic Issues**

**a. Lack of Standards**

***Inconsistent Security Practices:*** Lack of universal security standards on IoT networking devices causes uneven and frequently quite frail security deployments.

**b. Complex Ecosystems**

***Interoperability Issues:*** The diverse and complex nature of IoT ecosystems can result in compatibility issues and security gaps.

**8. Regulatory and Compliance Issues**

**a. Non-compliance**

***Failure to Meet Regulations:*** Organizations may fail to comply with relevant regulations and standards, resulting in vulnerabilities.

***Data Privacy Violations:*** Mishandling of user data leading to privacy breaches and legal ramifications.

# 4. Improvements and Enhancements Required for Upcoming IoT Applications

Upcoming IoT applications require improvements in several key areas including enhanced security measures, robust connectivity, efficient data processing, and seamless interoperability between devices.Prioritizing these aspects will enable more reliable, secure, and scalable IoT solutions across various industries [6].

a. Architecture and platform
b. Security and privacy
c. Connectivity and reliability
d. Data management and analytics
e. Developer experience and ecosystem
f. Operations and lifecycle management
g. Performance, cost, and sustainability
h. Industry-specific considerations
i. Malware Detection
j. Energy Efficiency

# 5. IoT Security using Blockchain

Consider a smart city with multiple IoT devices (sensors, cameras, smart meters),

all tied up in a network by a 5G network. Data integrity, unauthorized access and privacy protection are the main issues of concern.

**Blockchain Layer:** IoT data are stored on a permissioned Blockchain with the advantage of securing the data so that only preauthorized parties can modify or access the information.

**AI Layer:** AI algorithms scan the information line of abnormal behaviours, risk possible security attacks, and initiate effective actions.

**Integration:** Smart contracts can be designed to automate operations like authorization of data sharing and arrangement of responses to events on the basis of AI outcomes.

# 6. IoT Security Using Machine Learning

Another identified tool in enhancing the security of IoT is the use of machine learning (ML), which is becoming important because it can be used to achieve complex threat detection, anomaly identification, and auto-response to cyberattacks [3]. ML algorithms can also process the massive data of the IoT devices to detect patterns that will reveal malicious behaviour such as malware infection, DDoS attack, and unauthorized access.

**Specific ML Techniques Used in IoT Security:**

**a. Anomaly Detection Algorithms**

Algorithms like Isolation Forest, One-Class SVM, and Autoencoders are used to identify unusual patterns in IoT device behaviour.

**b. Classification Algorithms**

Algorithms like Decision Trees, Random Forests, and Support Vector Machines (SVM) are used to classify network traffic and identify malicious activity.

**c. Deep Learning Techniques**

Neural networks like Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) are used for complex pattern recognition and threat detection in IoT networks.

**d. Signature-based Detection**

ML can be used to analyse malware samples to determine the special features of this malware and signatures are created automatically to detect accuracy.

# 7. Open Issues, Challenges, and Future Research Directions

The following are open issues, challenges and future research topics in the use of ML in IoT security.

**a) Scalability and Performance -** The rate at which transactions are approved in a Blockchain is measured in transactions per second (TPS), and the low transaction speed of Blockchain is a major concern for several industries adopting the solution especially 5G. Most of the existing Blockchain solutions suffer from poor transaction rate and are not suitable for 5G networks. The throughput of the Blockchain is determined primarily by two factors. First, the consensus algorithms that determine how to reach an agreement to add the block. Second, the way Blockchain is designed i.e. private, public or consortium. A private or consortium Blockchain, which is most likely the case for 5G, is expected to achieve a higher transaction rate due to a controlled environment and limited participants involved in approving the transaction compared to public Blockchain [17].

**b) Security**- Although Blockchain is believed to resolve numerous security challenges when implementing the 5G network and the IoT, it has some security challenges associated with it. To give an example, consensus protocols as the primary constituent in the technologies of Blockchain, are more frequently under the fire of attackers. More so, when the attacker has access to controls over 50 percent of nodes in the Blockchain network also referred to as 51 percent attack, they can modify the blocks. The property of security of consensus algorithms has to be tested extensively then applied in a huge scale. Also, the smart contract that is important to the success of Blockchain could be vulnerable as a result of poor code [18]. Despite research works on protecting individual attacks on Blockchain in respect to various solutions, there is no standard solution that will be effective against such attacks.

**c) Networking and Storage**: Blockchain is computationally demanding and overhead intensive in reaching to a consensus. Such overhead may take up much space in the network. In some situations, there might be a scarcity of the resources thereby restricting the capacity to find a common ground quickly leading to the latency.

Moreover, the deal continues to append to the Blockchain hence causing escalated storage requirements. Some Blockchain applications demand that the node has the complete copy of the history of Blockchain transactions that cannot be achieved in devices that have limited resources. Some attempts have been made in this direction, such as, IoT has some prospects that can help to mitigate the problems due to scarcity of resources. Nevertheless, more study and approval are required to be implemented in 5G and beyond networks.[19]

**d) Selection of suitable Blockchain platform:** There have been several Blockchain platforms in the marketplace since the inception of Bitcoin. However, there are not sufficient experimental studies to report the suitability of one platform over the other one. This creates a challenge for adopting a suitable Blockchain platform on 5G networks which would be able to accommodate diverse requirements, such as performance, infrastructure cost, and data privacy, etc. This challenge cannot be tackled unless further experimental evidence could be provided. Hence, the Blockchain research community [17] needs to conduct more pilot research projects to explore and report the suitability of different Blockchain platforms for integration with 5G networks and beyond.

# 8. Conclusion

The combination of Blockchain and AI constitutes an encouraging scenario to solve the security and privacy issues of 5G-IoT systems. The case study is evidence that these technologies have so much potential to develop a secure, efficient, and smart framework of future IoT applications beyond 5G. Further studies are needed to streamline this combination and investigate how it can be used in many other scenarios in order to further prove its usefulness.

# References

1. Zhou, W., Zhang, Y., & Liu, P. (2018). The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *IEEE Internet of Things Journal, 6*(2), 1606-1616. https://ieeexplore.ieee.org/document/8386824

2. Singh, S., Singh, N. (2016). Blockchain: Future of financial and cyber security. *Proceedings of the 2nd International Conference on Contemporary Computing and Informatics (IC3I)*, pp. 463-467. https://ieeexplore.ieee.org/document/7918009

3. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks, 76*, 146-164. https://www.sciencedirect.com/science/article/abs/pii/S1389128614003971

4. Roman, R., Najera, P., & Lopez, J. (2011). Securing the Internet of Things. *Computer, 44*(9), 51-58. https://ieeexplore.ieee.org/document/6017172

5. Mollah, M. B., Zhao, J., & Niyato, D. (2020). A comprehensive review of blockchain and AI techniques in the smart grid: Past, present, and future. *IEEE Access, 8*, 150653-150670. https://ieeexplore.ieee.org/document/9090812

6. Hassija, V., Chamola, V., & Sikdar, B. (2020). A survey on IoT security: Application areas, security threats, and solution architectures. *IEEE Access, 7*, 82721-82743. https://ieeexplore.ieee.org/document/8742551

7. Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. *Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pp. 618-623. https://ieeexplore.ieee.org/document/7917634

8. M. N. Aman, K. C. Chua, & B. Sikdar. (2017). Mutual authentication in IoT systems using physical unclonable functions. *IEEE Internet of Things Journal, 4*(5), 1327–1340.

9. D. F. Rajesh Kandaswamy. (2018). Blockchain-based transformation. https://www.gartner.com/en/doc/3869696-blockchain-basedtransformation-a-gartner-trend-insight-report/

10. GSMA. (2019). Safety, privacy and security. https://www.gsma.com/publicpolicy/resources/safetyprivacy-security-across-mobileecosystem/

11. Flashpoint. (2018). Mirai botnet linked to dyn DNS DDoS attacks. https://www.flashpoint-intel.com/blog/cybercrime/mirai-botnet-linked-dyn-dns-ddos-attacks/

12. M. Frustaci, P. Pace, G. Aloi, & G. Fortino. (2018). Evaluating critical security issues of the iot world: present and future challenges. *IEEE Internet of Things Journal, 5*(4), 2483–2495.

13. Y. Yang, L. Wu, G. Yin, L. Li, & H. Zhao. (2017). A survey on security and privacy issues in internet-of-things. *IEEE Internet of Things Journal, 4*(5), 1250–1258.

14. Smarthomeblog. (2019). How to make your smoke detecter smarter. https://www.smarthomeblog.net/smart-smoke-detector/

15. Dai, H. N., Zheng, Z., & Zhang, Y. (2019). Blockchain for Internet of Things: A survey. *IEEE Internet of Things Journal, 6*(5), 8076-8094. https://ieeexplore.ieee.org/document/8731639

16. Reis, M. (2025). *Blockchain-enhanced security for 5G edge computing in IoT. Computation*. https://doi.org/10.3390/computation13040098

17. M. Tahir, M. H. Habaebi, M. Dabbagh, A. Mughees, A. Ahad, & K. I. Ahmed. (2020). A review on application of blockchain in 5G and beyond networks: Taxonomy, field-trials, challenges and opportunities. *IEEE Access, 8*, 115876-115904. doi:10.1109/ACCESS.2020.3003020.

18. M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, & H. Janicke. (2019). Blockchain technologies for the Internet of Things: Research issues and challenges. *IEEE Internet Things J., 6*(2), 2188–2204.

19. R. Alexander. (2018). *Iota-Introduction to the tangle technology: Everything You need to know about the revolutionary blockchain alternative*. Independently Published.