International Innovative Research Journal of Engineering and Technology
Vol. 12, Issue. 1, Sep 2026, pp. 1~13
ISSN: 2456-1983, DOI: 10.32595/iirjet.org/v12i1.2026.251

Blockchain-Enabled Artificial Intelligence System for Real-Time Threat Detection in IoT Networks

Gofurjanov Ibrokhimjon Ilkhomjon ugli[1], Azizov Azizbek Sabitkhanovich[2]

[1]Associate Professor of Information Technology, Faculty of Business Administration, Turan International University, Namangan, Uzbekistan.
[2]Director of the Department of Scientific Affairs and Innovations, Faculty of Business Administration, Turan International University, Namangan, Uzbekistan.

Article Info

Article History:

Received Jul 05, 2026
Revised Aug 08, 2026
Accepted Sep 05, 2026

Keywords:

IoT,
Artificial Intelligence,
Blockchain,
Real-Time Threat Detection,
Cybersecurity

ABSTRACT

The attack surface for data manipulation, unauthorized access, and distributed denial of service (DDoS) is expanding due to the continuous expansion of connected Internet of Things (IoT) devices. The Centralized security solutions are hazards to privacy and single points of failure when managing the Internet of Things' size and variety. This article suggests a Blockchain-Enabled Artificial Intelligence System (BCAIS) for Real-time Threat Detection in IoT Networks to provide decentralized trust, improved data integrity, and transparent security event monitoring. To enable real-time anomaly detection and automated reaction, the suggested model combines machine learning-based threat identification with blockchain-based security event monitoring. The methodology is designed to ensure tamper-resistant security event records while identifying known and undiscovered dangers across heterogeneous IoT domains. The model's performance is evaluated using accuracy, precision, recall, F1-score, and detection latency. This technology enhances cyber resilience in critical sectors including manufacturing, energy, and infrastructure, where maintaining operational continuity and safety depends on timely and dependable attack responses by enabling quick, comprehensible, and low-latency intrusion detection directly on edge devices.

Corresponding Author:

Gofurjanov Ibrokhimjon Ilkhomjon ugli,
Associate Professor of Information Technology,
Faculty of Business Administration,
Turan International University, Namangan, Uzbekistan.

1. INTRODUCTION

The Internet of Things (IoT) is a crucial technology for establishing connections between physical items, sensors, actuators, and intelligent systems via communication networks. IoT applications are increasingly being used in healthcare, smart homes, industrial automation, transportation, agriculture, and smart city infrastructures. Real-time data gathering and automated decision-making are made possible by the ongoing interaction between diverse and resource-constrained devices [1]. Artificial intelligence and Internet of Things technologies have been

incorporated into real-time applications in recent decades to process and aggregate data from external sources, improving the responsiveness and prediction of heterogeneous services. IoT devices regularly generate network and activity data that need to be handled proficiently to detect unusual communication behaviors and possible security threats [2, 3].

In recent years, specialists have focused increasingly on the application of blockchain, AI, and IoT security systems. Real-time adaptation and adaptability to change are made possible by AI, especially machine learning (ML), which is used to carry out predictive analytics and quickly detect anomalies. The security data produced by an AI system still needs to be reliably stored and verified, even though AI can enhance threat detection. This need can be met by blockchain technology's decentralized, tamper-resistant data management [4].

Due to their limited resources, many IoT devices lack the computing capacity needed to operate blockchain and AI applications. For example, it is difficult to deploy computationally expensive blockchain protocols and AI models since a simple IoT device frequently lacks the CPU, memory, and electricity to support them. Alternatively, by distributing the processing load among multiple devices positioned at the network's edge, the most recent advancements in edge computing technologies aim to address these security concerns. Additionally, new blockchain protocols are designed to function in Internet of Things settings. These protocols are designed to be extremely specialized and require minimal resources in order to guarantee high-level security [5]. Lightweight blockchain protocols in Internet of Things devices have been the subject of recent research. It has been demonstrated that lightweight blockchain protocols are intended to reduce the overhead brought on by these IoT protocols at the expense of performance and security [6].

Consequently, the combination of edge computing, blockchain, and AI offers complementary security capabilities. Blockchain can offer decentralized trust and tamper-resistant security records, edge computing can enable low-latency processing, and AI can handle intelligent threat identification and categorization [7]. Real-time threat detection in IoT is still a difficult research challenge, nevertheless. Furthermore, the implementation of blockchain shouldn't result in excessive resource consumption or transaction delays that impair real-time security operations. The performance of the proposed system may be evaluated using metrics such as accuracy, precision, recall, F1-score, false-positive rate, detection latency, blockchain transaction latency, and resource usage. By combining edge-oriented computing, blockchain, and artificial intelligence, the research aims to provide a practical and scalable way to improve the security and reliability of IoT networks against evolving cyber threats.

Despite these improvements, existing techniques encounter obstacles in accomplishing the simultaneous requirements of real-time threat detection, quick processing, effective use of resources, and a reliable security-event management system. AI-based models focus on detecting suspicious/ illegal behavior, whereas blockchain-based methods prioritize data reliability and the ability to monitor it.

This study suggests a Blockchain-Enabled Artificial Intelligence System for Real-Time Threat Detection in IoT Networks to overcome the drawbacks of existing IoT security techniques. The suggested design is evaluated using performance criteria such as resource utilization, blockchain transaction latency, accuracy, precision, recall, and F1-score.

2. LITERATURE REVIEW

Abdalgawad [8] describes how companies can identify potential threats and take prompt action by using machine learning models to identify cyberattacks. The suggested approach combines blockchain technology with artificial intelligence to identify all irregularities and safely record them in an immutable ledger. The approach extremely enhances data integrity and detection accuracy since each possible threat identified by the AI is immediately and permanently stored. Abdalgawad further emphasizes that AI's influence on cybersecurity goes well beyond simple threat identification.

To determine attacks in Internet of Things (IoT) networks, [9] proposed a new approach to deal with the problem of attacks initiated by IoT devices. The autoencoder was then utilized to identify anomalies in IoT communications. The dataset they used to evaluate their proposed techniques was the Internet of Things-based botnet attacks Bashlite and Mirai. However, the used datasets are also present in a variety of compromised IoT network devices. In their research, they showed that the proposed approach may detect cyberattacks in IoT network devices with exceptional performance results.

According to Menon [10] the concept of cognitive cities requires the implementation of networked systems that gather, process, and analyze enormous amounts of data in real-time in order to facilitate efficient urban management. These systems are used in many different fields, such as public safety, healthcare, energy management, and smart transportation. However, they confront significant obstacles in preserving system resilience, secure communication, and data integrity. Because cyberattacks on these interconnected networks could severely impact privacy, public safety, and general urban operations, blockchain technology has emerged as a powerful solution. By utilizing an immutable, decentralized ledger, blockchain effectively safeguards data and transactions within cognitive city environments.

Abdullah Ayub Khan et al [11] suggested the serverless consortium fog and edge computing infrastructure security solution provided by blockchain. This article's main objective is to compile the most recent studies and surveys on the state of the art in edge distributed computing, covering fog and edge, and compute outsourcing. The author described a serverless distributed outsourced computing architecture based on the Hyperledger Sawtooth blockchain. This theoretical architecture-based solution offers excellent data security with respect to transparency, integrity, provenance, and privacy protection while safely storing outsourced computational ledgers in immutable storage. This article also highlights differences between the proposed taxonomy and the current system based on a number of characteristics, including system security and privacy.

Hang and Kim [12] proposed a decentralized system that provides fast and safe information transfer. The IoT blockchain network in Docker created smart contracts using Hyperledger Playground, and values were stored in CouchDB. Temperature and humidity sensors were installed on the Raspberry PI IoT device server. Apache WebApp was used to host the blockchain web application. IoT servers acted as a gateway, and the IoT device utilized was not a part of the blockchain network. To address issues with scalability, identification, and data security, a novel approach was put out for creating and implementing a decentralized IoT platform. However, inquiries concerning blockchain transactions were directed toward the IoT server.

3. METHODOLOGY

The suggested method combines monitoring of the IoT network, processing of data, detecting threats using AI, and recording security events using blockchain technology forming a single process, as illustrated in Figure 1. The aim is to identify threats immediately at the moment keeping security records intact and traceable.

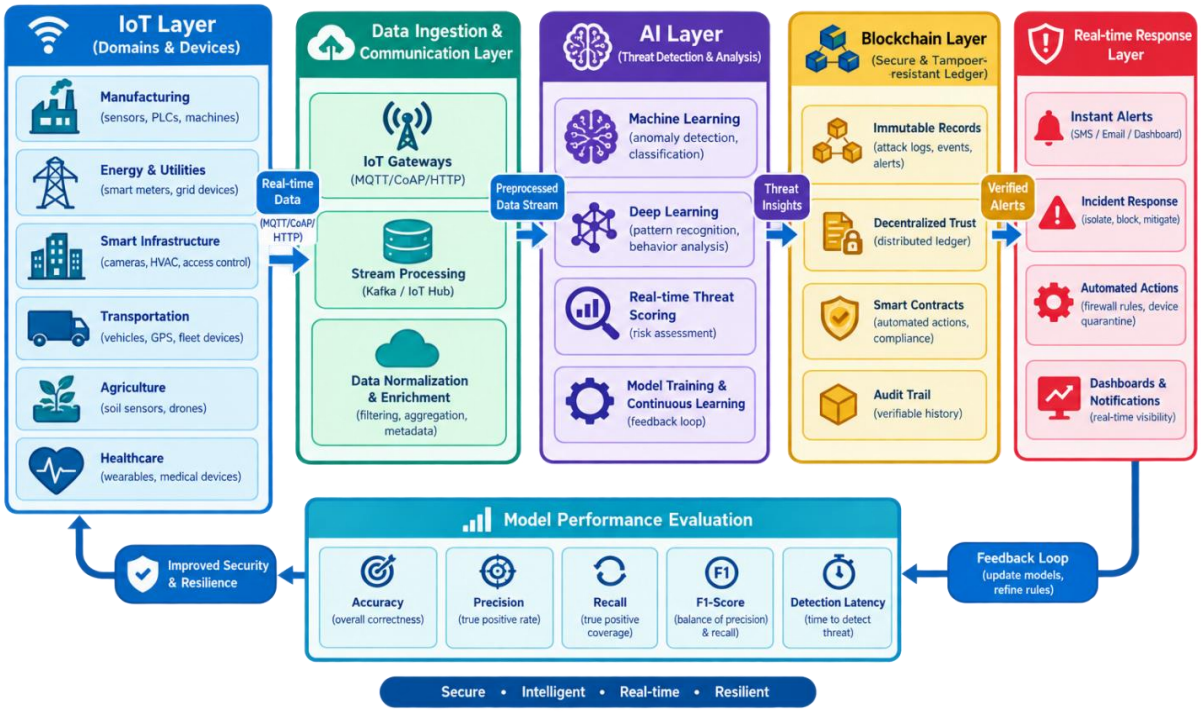


Figure 1. The Proposed IoT-AI-Blockchain Architecture

The procedure suggested commences with the process of consistently gathering the network traffic created by IoT devices. Figure 1 illustrates the proposed IoT-AI-Blockchain architecture for real-time threat detection and response. Communications' data produced by sensors, smart appliances, cameras, actuators, and other interconnected devices encompasses both the regular events and the anomalous ones. The data is gathered so that its properties become evident, and it can be refined by preventing missing values, duplicate records, wrong features, or inconsistent values in the data. Numerical characteristics of the input data are standardized to one general value, which allows receiving appropriate descriptors of the communication behavior, packet features, amount of traffic, connection structure, and other network parameters. The detection layer that is based on an AI system examines the features of the IoT network that have been captured in order to find the unexpected behavior of the network. The chosen machine learning technique is used to classify the incoming network data as either not threatening or threatening. Such an approach requires the model to be trained on the datasets of labeled network traffic and to be assessed with relevant classification metrics. The output given by the model states whether the traffic received by the network is normal or dangerous. The prediction can be represented as:

$$\hat{y} = f_{\theta}(X) \tag{1}$$

where x, represents the extracted network features, f_{θ} represents the trained AI model, and $\hat{y}$ represents the predicted class.

A threshold-based decision-making procedure may be used to determine whether the observed behavior may be considered suspicious. If the threat probability exceeds a predefined threshold, the system generates a threat event. This enables the proposed architecture to enable detection in nearly real time.

Blockchain technology is used to record crucial detection information when a danger is detected. The system can save the detection result, timestamp, and device identifier on the blockchain instead of storing all of the raw IOT traffic.

A simplified blockchain relationship is :

$$B_i = Hash(B_i||D_i||T_i) \quad (2)$$

By creating a connection between subsequent blocks, this aids in maintaining the integrity and traceability of security records.

Security recording and verification processes can be automated with smart contracts. Upon receiving a legitimate threat-detection event, the smart contract can confirm the necessary details and start the associated blockchain transaction.

The alert and monitoring layer shows the security event detection via a monitoring dashboard. Security administrators can see the type of threat and other relevant information. This provides a centralized view of the security situation of the IoT environment.

The performance of the proposed methodology is evaluated using multiple metrics rather than accuracy alone. The major metrics include accuracy, precision, recall, F1-score, false-positive rate, detection latency, and resource utilization. The primary metrics include accuracy, precision, recall, F1-score, false-positive rate, detection delay, and resource consumption.

The false-positive rate can be calculated as:

$$FRR = \frac{FP}{FP+TN} \quad (3)$$

The detection latency can be represented as

$$L_d = T_{alert} - T_{input} \quad (4)$$

Where T_{alert} is the time at which the alert is generated and T_{input} is the time at which the corresponding network data is received.

3.1 Data Normalization

IoT network characteristics can exhibit different numerical ranges. Data normalization converts these values into a common range, usually between 0 and 1. This makes it possible to keep the uniformity of the input features before being provided to the AI model.

$$X_{norm} = \frac{X-X_{min}}{X_{max}-X_{min}} \quad (5)$$

- X = original feature value
- X_{min}= minimum feature value
- $X_{\max}$ = maximum feature value
- X_{norm}= normalized feature value

3.2 AI Threat Detection

The trained AI model receives the preprocessed network features. After analyzing the input, the model generates a predicted class.

$$\hat{Y} = f_{\theta}(X') \tag{6}$$

- X'= preprocessed network data
- f_{θ}= trained AI model
- $\theta = \text{parameters of the model}$
  $\hat{y}$ = predicted output

For instance,

$$\hat{Y} \in \{\text{Normal, Threat}\}$$

Threat Decision

$$D = \begin{cases} 1, & P(Threat|X') \geq T \\ 0, & P(Threat|X') < T \end{cases} \tag{7}$$

A threshold (T) is used to make the final decision.

- D=1 threat detected
- D=0 normal traffic
- T= threshold predefined detection

Blockchain Record

$$B_i = Hash(B_i||D_i||T_i)$$

Once a threat has been identified, crucial detection data can be entered into the blockchain. A cryptographic hash connects the current block to the prior block.

- B_i = current blockchain block
- B_{i-1}= previous block
- D_i = detection result
- T_i = timestamp
- $Hash$ = cryptographic hash function
- || = concatenation

This ensures the security records' traceability and integrity.

3.3 Accuracy

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \tag{8}$$

Accuracy is defined as the proportion of correctly classified network records among all tested records.

3.4 Precision

$$Precision = \frac{TP}{TP+FP} \tag{9}$$

Precision shows the proportion of traffic data classified as threats that were in fact threats. Fewer false alarms result from increased precision.

3.5 Recall

$$Recall = \frac{TP}{TP+FN} \tag{10}$$

Recall measures the system's ability to identify actual threats. A higher recall suggests that fewer real threats are missed.

3.6 F1-Score

$$\mathrm{F1} = 2 \times \frac{Prescision \times Recall}{Precision + Recall} \tag{11}$$

The F1-score integrates recall and precision into a single metric. It is helpful when it's crucial to identify dangers and lower false alarms.

3.7 False Positive Rate

$$FPR = \frac{FP}{FP+TN} \tag{12}$$

The false positive rate is the proportion of normal IoT traffic that is incorrectly identified as a threat. When the value is lower, there are fewer unnecessary notifications.

3.8 Detection Latency

$$L_d = T_{alert} - T_{input} \tag{13}$$

The amount of time it takes the system to identify a threat and issue an alarm is measured by detection latency.

- T_{input} = time when network data enters the detection system
- T_{alert} = time when the alert is generated
- L_d = detection latency

This method is very crucial for achieving your goal of real-time threat detection.

4. PERFORMANCE COMPARISON OF IoT THREAT DETECTION APPROACHES

The comparative results between Traditional Method, AI-based Method, Blockchain-based Method, and the introduced BCAIS method. The measuring metrics for evaluation are accuracy, precision, recall, F1 score and detection latency. According to the obtained results, the technique BCAIS delivers the highest accuracy of 96%, precision of 93%, recall of 92% and F1 score of 95%. Hence, the proposed BCAIS method can enhance the effectiveness of detection of threats and their classification in comparison with other methods. Moreover, the technique shows detection latency of 190 in contrast to 400 of Traditional Method, 250 of AI-based technique and 340 of Blockchain-based Method. It is/ is not noteworthy because the lower the detection latency the quicker the threat is detected. To conclude, results in Table 1 reveal that the method proposed can ensure better detection quality and faster response to security threats.

Table 1. Performance Comparison of Traditional, AI-Based, Blockchain-Based, and Proposed BCAIS Approaches for IoT Security

Performance Metrics	Traditional	AI-based	Blockchain	BCAIS
Accuracy	88%	92%	90%	96%
Precision	76%	87%	82%	93%
Recall	74%	85%	80%	92%

Performance Metrics	Traditional	AI-based	Blockchain	BCAIS
F1-score	75%	86%	81%	95%
Detection latency	400%	250%	340%	190%

The accuracy comparison demonstrates how well each method distinguishes between legitimate and dangerous IoT network traffic, as shown in Figure 2. Better overall categorization performance is indicated by a higher accuracy.

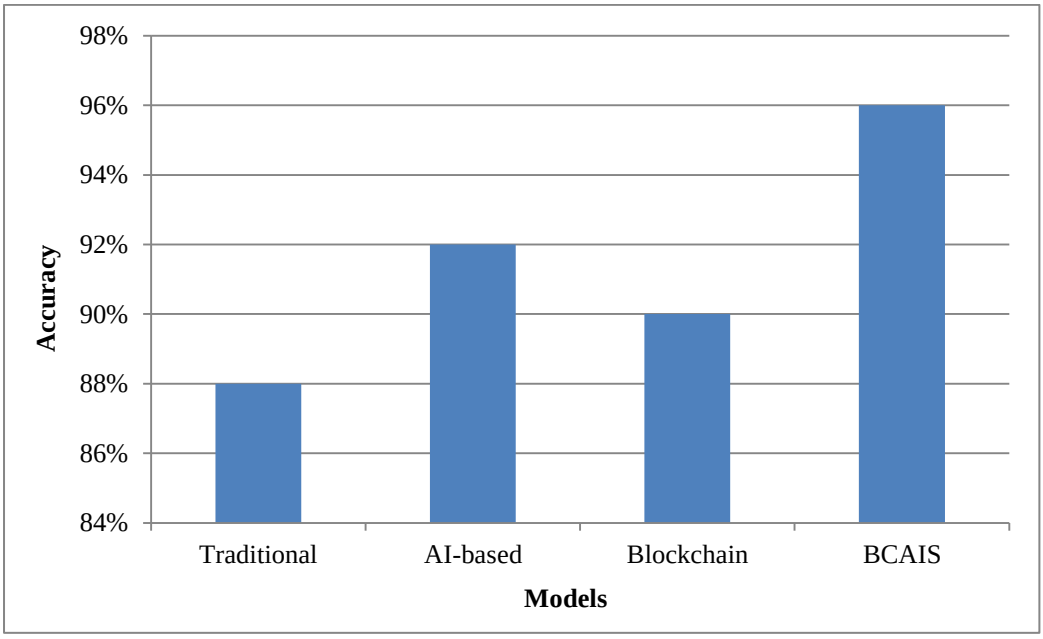


Figure 2. Comparative Analysis of Accuracy among Traditional, AI-Based, Blockchain-Based, and Proposed BCAIS Approaches for IoT Threat Detection

Accuracy is used to determine the performance of a system in classifying both uncertain and harmful traffic on IoT networks. In Figure 2 comparison with Traditional techniques (which provide an accuracy of 88%), AI techniques as well as Blockchain techniques provide an accuracy of 92% and 90%, respectively. The accuracy performance of the suggested BCAIS technique surpasses the performance of the mentioned approaches due to its accuracy of 96%, which is 8% more than that of the Traditional approach.

Precision is a measure of how well the system detects real threats among the traffic that has been labeled as such, as compared in Figure 3. Fewer false threat alarms result from improved precision.

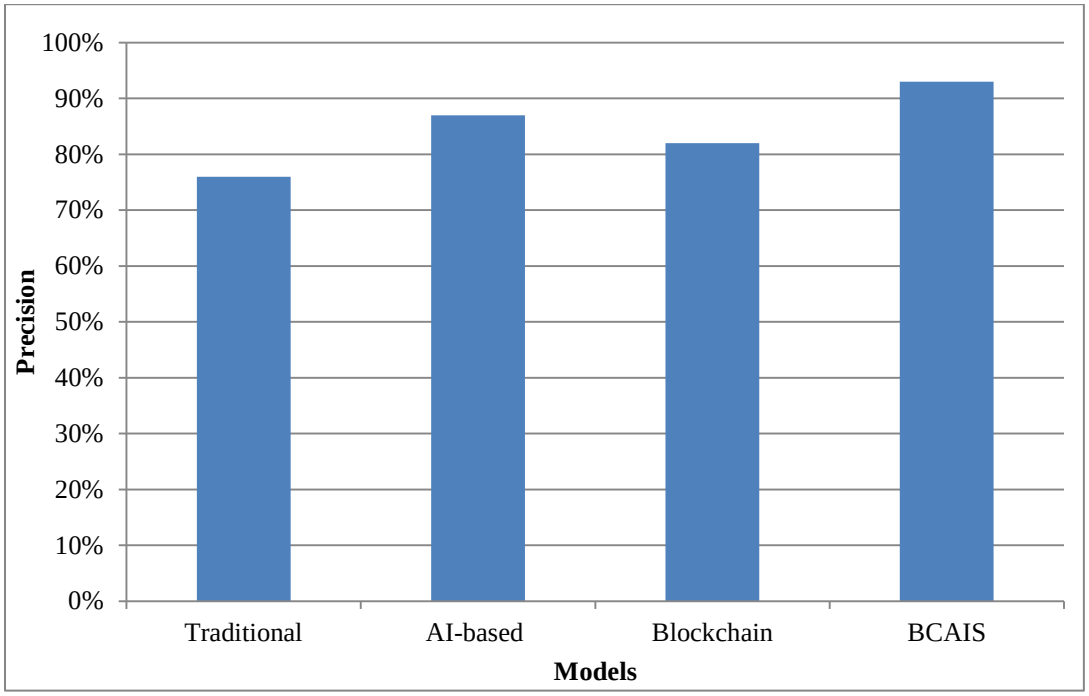


Figure 3. Comparative Analysis of Precision among Traditional, AI-Based, Blockchain-Based, and Proposed BCAIS Approaches for IoT Threat Detection

Precision determines the percentage of detected threats that are truly malicious. The higher the precision, the fewer false positive classification of attacks there are. As seen in Figure 3, the Traditional method provides accuracy of 76%, compared to 87% of the AI-based method and 82% of the Blockchain-based method. Finally, the proposed BCAIS method achieves the highest accuracy of 93%, which brings 17 additional points of precision in comparison with the implementation of the Traditional method and proves that BCAIS can detect malicious traffic more effectively with elimination of false alarms.

Recall measures the system's capacity to identify actual dangers within the Internet of Things network, as compared in Figure 4. Fewer risks are overlooked when recall is strong.

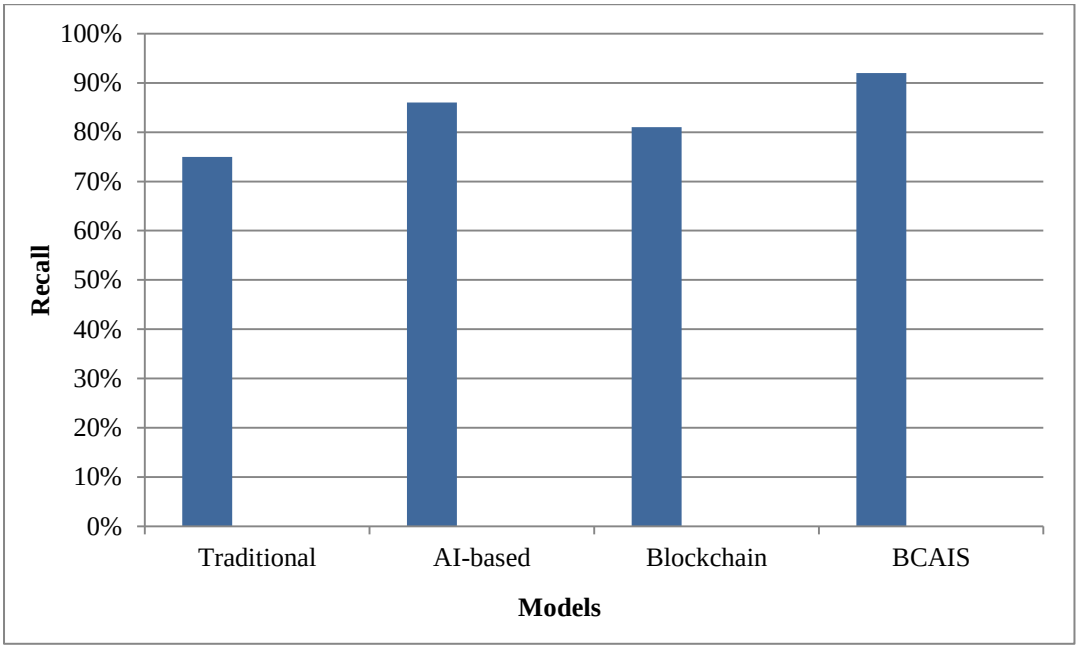


Figure 4. Comparative Analysis of Recall among Traditional, AI-Based, Blockchain-Based, and Proposed BCAIS Approaches for IoT Threat Detection

Recall assesses the percentage of real harmful traffic cases correctly recognized by the detection system. A high recall value means fewer genuine dangers are left out of consideration. In Figure 4, the Traditional method has 74% recall compared to 85% recall of the AI-based method and 80% of the Blockchain technology approach. The proposed BCAIS method has the maximum recall value of 92% giving the rise of 18 percentage points in connection with the Traditional method.

Precision and recall are combined into one metric called the F1-score, which is compared in Figure 5. It offers a fair assessment of the threat-detection performance, especially when both missed threats and false positives are significant.

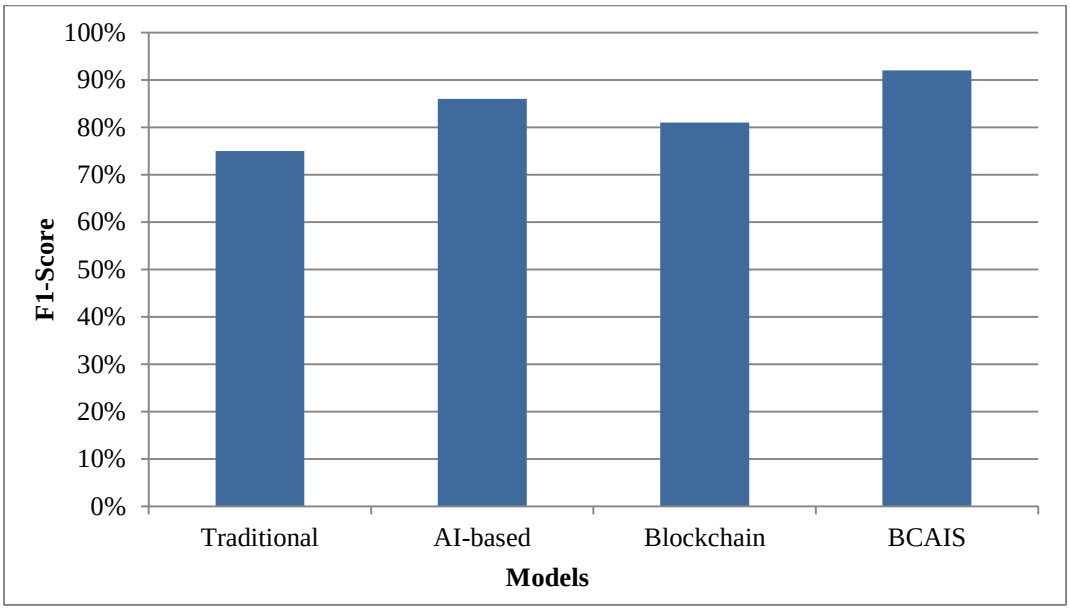


Figure 5. Comparative Analysis of F1-Scores among Traditional, AI-Based, Blockchain-Based, and Proposed BCAIS Approaches for IoT Threat Detection

The F1-score is the harmonic mean of precision and recall, thereby representing a single measure. This measure gives an overall assessment of the capability of a system to detect threats. While the F1-score also accounts for false positives and false negatives, credit has to be given to the F1-score as shown in Figure 5. The use of the traditional method has yielded an F1-score of 75%, while the F1-scores for AI-based and Blockchain-based methods are 86% and 81% respectively. The BCAIS method, which is the main method proposed in this paper, achieved an F1-score of 95%, thus indicating the best performance concerning precision and recall among the four methods. This makes the method 20% better than the traditional method reported.

Detection latency is the time interval between receiving network activity and generating a threat alert, as compared in Figure 6. Real-time threat detection is accelerated with lower latency.

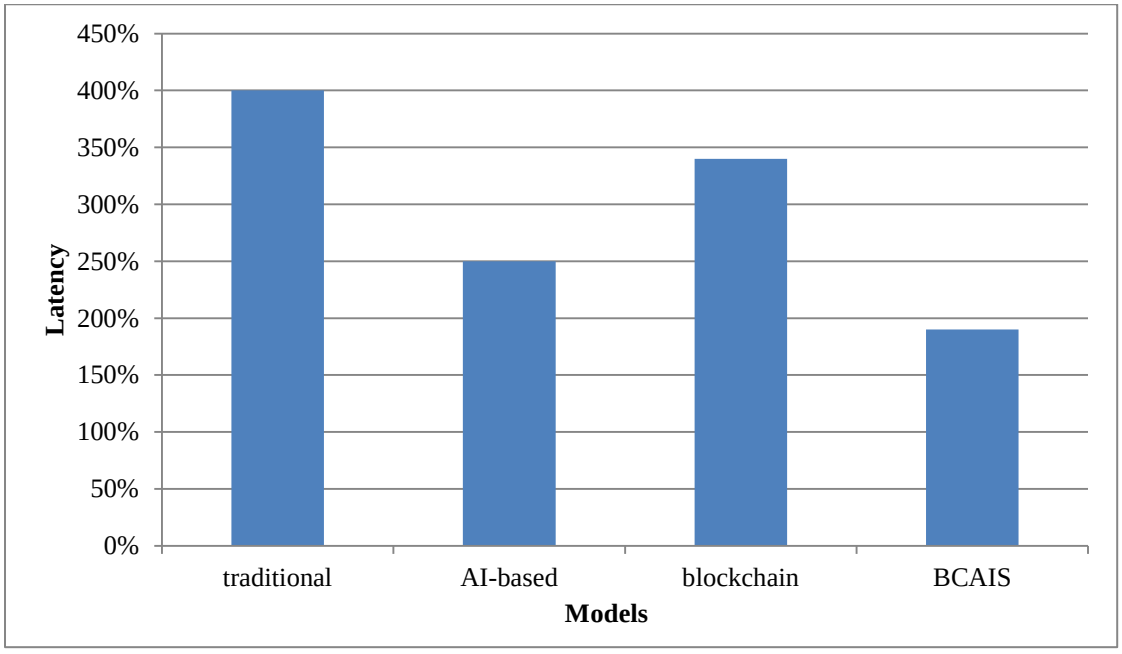


Figure 6. Comparative Analysis of Detection Latency among Traditional, AI-Based, Blockchain-Based, and Proposed BCAIS Approaches for IoT Threat Detection

Detection latency refers to the time required for a system to process network activity and generate a threat alert. Lower latency indicates faster threat detection and is particularly important for real-time IoT security applications. As shown in Figure 6, the Traditional approach records a detection latency of 400, while the AI-based and Blockchain-based approaches record 250 and 340, respectively. The proposed BCAIS approach records the lowest latency of 190, indicating faster threat detection than the other approaches. Compared with the Traditional approach, BCAIS reduces detection latency by 52.5%, assuming all values are measured in the same time unit. This suggests that the proposed approach can improve the responsiveness of IoT security systems.

4.1 Discussion

The suggested Blockchain-Enabled Artificial Intelligence System (BCAIS) includes IoT network monitoring and data preprocessing as well as AI-based threat detection and blockchain-based security event documentation. Through the means of AI technology, the system determines network characteristics to recognize possible dangerous activities. As soon as the danger is discovered, the system saves the related information, including the data regarding the detection and the date and time, into the blockchain. This ensures the integrity and traceability of the security records that are kept and makes it challenging for unauthorized parties to alter previously recorded detection information. The performance of the proposed framework may be evaluated using

accuracy, precision, recall, F1-score, false-positive, detection latency, and blockchain transaction latency. Precision evaluates the accuracy of threats that have been recognized, recall evaluates the capacity to identify real threats, and accuracy evaluates the overall correctness of the detection process. However, the false-positive rate illustrates how often regular traffic is mistakenly categorized as hazardous , the F1 score offers a combined evaluation of recall and precision.

To determine the additional processing time needed to safely record detection events, blockchain transaction latency can also be investigated. Thus, the resultant framework shows how integrating blockchain-based record keeping, AI-based detection, and real-time monitoring may result in a comprehensive security mechanism for IoT networks.

5. CONCLUSION

The Blockchain-Powered Artificial Intelligence System (BCAIS) proposed intends to strengthen the security of IoT networks by integrating artificial intelligence-based threat detection with blockchain-based security event recording techniques. The proposed approach includes gathering network traffic, preprocessing data, extracting features, identifying threats, and recording the findings securely. This comprehensive methodology will help in recognizing any suspicious activity on the network while reinforcing the trustworthiness and tracking of security records.

Real-time alarm and monitoring systems, which rapidly notify administrators of detected dangers, further increase the framework's value. The effectiveness of the proposed architecture may be demonstrated by experimental evaluation utilizing measures such as accuracy, recall, F1-score, false-positive rate, and detection delay. The overall design distinctly differentiates between the monitoring layer's timely security awareness, Blockchain's reliable security record management, and AI's intelligent threat detection. In future work, the research will investigate the performance of the new framework under real IoT conditions and various kinds of attacks. Further work will analyze the performance of the detection, delay in processing, blockchain burden, and consumption of resources on IoT devices with limited resources.

REFERENCES

[1] Neto, E. C. P., Dadkhah, S., Ferreira, R., Zohourian, A., Lu, R., & Ghorbani, A. A. (2023). CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment. *Sensors*, *23*(13), 5941. https://doi.org/10.3390/s23135941

[2] Duan, S., Wang, D., Ren, J., Lyu, F., Zhang, Y., Wu, H., & Shen, X. (2022). Distributed artificial intelligence empowered by end-edge-cloud computing: A survey. *IEEE Communications Surveys & Tutorials*, *25*(1), 591-624.

[3] Alzoubi, M. M. (2025). Investigating the synergy of Blockchain and AI: enhancing security, efficiency, and transparency. *Journal of Cyber Security Technology*, *9*(3), 227-255.

[4] Ruzbahani, A. M. (2024). Ai-protected blockchain-based iot environments: Harnessing the future of network security and privacy. *arXiv preprint arXiv:2405.13847*.

[5] Li, X., Liu, Y., Ji, H., Zhang, H., & Leung, V. C. (2019). Optimizing resources allocation for fog computing-based internet of things networks. *IEEE Access*, *7*, 64907-64922.

[6] Khan, D., Jung, L. T., & Hashmani, M. A. (2021). Systematic literature review of challenges in blockchain scalability. *Applied Sciences*, *11*(20), 9372.

[7] Kaushik, D., Gulia, P., Gill, N. S., Yahya, M., Shukla, P. K., & Shreyas, J. (2026). Synergizing blockchain and AI to fortify IoT security: a comprehensive review. *Artificial Intelligence Review*, *59*(2),41.

[8] Abdalgawad, N., Sajun, A., Kaddoura, Y., Zualkernan, I. A., & Aloul, F. (2021). Generative deep learning to detect cyberattacks for the IoT-23 dataset. *Ieee Access*, *10*, 6430-6441.

[9] Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., & Elovici, Y. (2018). N-baiot—network-based detection of iot botnet attacks using deep autoencoders. *IEEE Pervasive Computing*, *17*(3), 12-22.

[10] Menon, V. G., Khosravi, R., Jolfaei, A., & Kumar, A. (2022). Cognitive smart cities: Challenges and trending solutions. *Expert Systems*, *39*(5), 1.

[11] Khan, A. A., Laghari, A. A., Baqasah, A. M., Alroobaea, R., Almadhor, A., Sampedro, G. A., & Kryvinska, N. (2024). Blockchain-enabled infrastructural security solution for serverless consortium fog and edge computing. *PeerJ Computer Science*, *10*, e1933.

[12] Hang, L., & Kim, D. H. (2019). Design and implementation of an integrated iot blockchain platform for sensing data integrity. *sensors*, *19*(10), 2228.