International Information and Engineering Technology Association
Advancing the World of Information and Engineering

International Journal of Safety and Security Engineering
Vol. 15, No. 8, August, 2025, pp. 1611-1625
Journal homepage: http://iieta.org/journals/ijsse

Integrated Framework for Real-Time Cyber Threat Detection and Mitigation in IoT and Healthcare Systems Using Deep Learning and Blockchain

Zainab Qahtan Mohammed[1*], Chasib Hasan Abooddy[1], Omar Hatem Zaidan[2]

[1] Basic Education College, University of Diyala, Baqubah 32001, Iraq
[2] Department of Scholarships and Cultural Relations, University of Diyala, Baqubah 61209, Iraq

Corresponding Author Email: Zainabkahtan@uodiyala.edu.iq

https://doi.org/10.18280/ijsse.150807

Received: 6 April 2025
Revised: 5 June 2025
Accepted: 12 June 2025
Available online: 31 August 2025

Keywords:
AI, blockchain, IoT security, deep learning, real-time threat detection

ABSTRACT

This study proposes a new model that integrates artificial intelligence (AI), deep learning (DL), and blockchain technology with the goal of enhancing the Internet of Things (IoT) ecosystems' security threats mitigation and detection mechanisms. The model solves the specific security problems in these fields by proposing a DL-based real-time threat detection AI model. Moreover, blockchain technology is applied to ensure data integrity and provide tamper-proof records. The model is tested thoroughly on both IoT and healthcare settings to ensure that it is streamlined and effective in shielding critical systems from security threats.

1. INTRODUCTION

1.1 Background on IoT security challenges

Industries have changed because of the automation of data and the ability of different devices to communicate with each other via the Internet of Things (IoT). A multitude of different devices are also interconnected, which makes it easier for attackers and hackers to infiltrate and use every device as a possible cyber weapon. IoT devices mostly use the same hardware and software systems, which causes a lack of differentiation across integrated systems. The lack of difference across integrated systems simplifies the mass deployment of devices, but that also means that there is a universal security inadequacy across the devices. In other words, if one device of a specific type or one version of a device has a security gap, thousands or millions of other devices of the same type or version are also compromised. A perfect example of this is the 2016 Mirai botnet attack, where 600,000 devices were infected worldwide because of default credentials in IoT routers and cameras [1].

An increased attack surface and a lack of suitable responsive security measures in resource-scarce situations, such as in the healthcare or industrial sectors, are a few of the negative impacts that a homogeneous system breakdown may incur.

These systems have been in the spotlight as a result of security system weakness, for example, the lack of encryption in several IoT systems, as a result of their limited computational resources. Such an adverse security resource scenario may be harnessed to devise effective and less burdensome alternative security measures. Due to the rapid growth of IoT systems, reliance on static security measures to formulate policies regarding control and movement of \ device systems should be loosened. This increased movement aggravates the challenges of maintaining system integrity, and weak centralized control aggravates compromise and risk. Integrating security will entail the coordination and use of contemporary technology such as blockchain and artificial intelligence (AI) [2].

1.2 Importance of detecting threats in real-time

To adapt to the digital IoT ecosystems, the need for instantaneous threat detection and mitigation to balance the cyber-attack is crucial. As illustrated in Figure 1, IoT's sensor networks and digital devices operate unattended and bring a new unique set of challenges. These environments are challenges for an all-in-one digital protection security. Most incident response automation tries to tackle to reduce and contain the risks, security, and digital protection the opportunistic attacks within seconds. This is more multi-dimensional and systemic. Along with system enhancement to avert damage and augmented protection, it aids in vision and systemic response. Rapid and successful damage containment is also critical to the protection and confidentiality of the information. The fast containment and response to probable cybersecurity risks in the health and critical national infrastructure are extremely crucial, as the data breaches are more catastrophic compared to others. Smart grid environments represent a clear example of such critical infrastructure, where blockchain-based integrity and trustworthy event logging can significantly strengthen resilience against real-time cyber threats [3].

The additional value comes from the immutable audit logs provided by the AI-enhanced blockchain technology, which also fortifies the system by providing audit trails for transactions and data to which users cannot alter. These organizations can easily demonstrate the adaptive and mitigating security mechanisms in place to respond to the system vulnerabilities as digital security is created in real time [4].

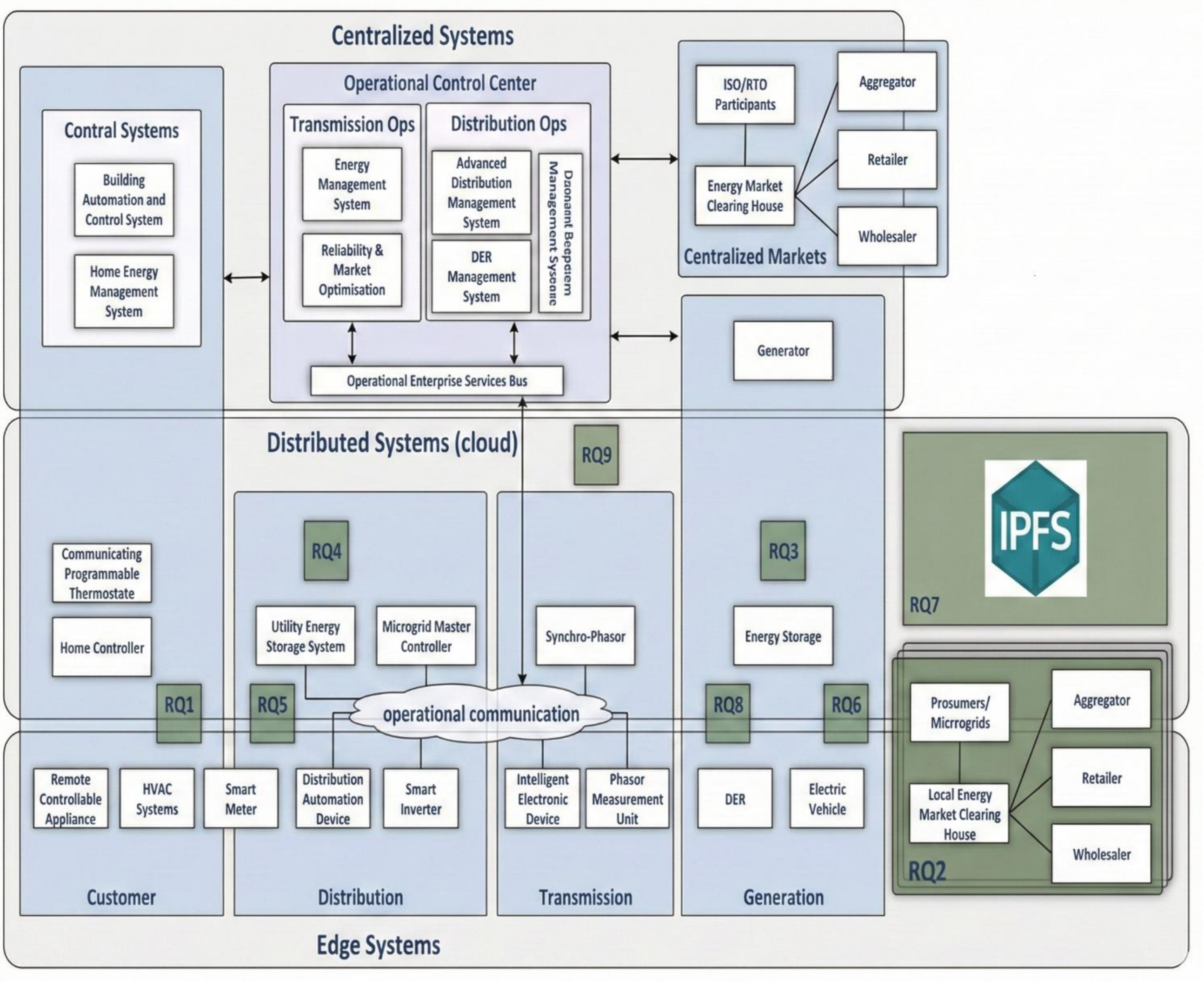

Centralized Systems
Contral Systems
Building Automation and Control System
Home Energy Management System
Operational Control Center
Transmission Ops
Energy Management System
Reliability & Market Optimisation
Distribution Ops
Advanced Distribution Management System
DER Management System
Dzonant Beepetem Management Syscaпe
Operational Enterprise Services Bus
ISO/RTO Participants
Energy Market Clearing House
Aggregator
Retailer
Wholesaler
Centralized Markets
Generator
Distributed Systems (cloud)
RQ9
RQ4
RQ3
RQ7
IPFS
Communicating Programmable Thermostate
Home Controller
Utility Energy Storage System
Microgrid Master Controller
Synchro-Phasor
Energy Storage
RQ1
RQ5
operational communication
RQ8
RQ6
Prosumers/ Micrrogrids
Local Energy Market Clearing House
Aggregator
Retailer
Wholesaler
RQ2
Remote Controllable Appliance
HVAC Systems
Smart Meter
Distribution Automation Device
Smart Inverter
Intelligent Electronic Device
Phasor Measurement Unit
DER
Electric Vehicle
Customer
Distribution
Transmission
Generation
Edge Systems

Figure 1. A model conceptually based on the NIST framework proposal

1.3 Overview of the integrated framework

This architecture leverages the combination of blockchain, AI, and deep learning (DL) technology and specifically addresses the relevant security challenges of IoT. Thanks to the peer-to-peer blockchain, the system is able to maintain transparency as well as confidentiality. A blockchain environment contains security challenges by minimizing the amount of exploitable primary datasets and the chances of single points of failure. Threat detection is accelerated by DL algorithms specialized for monitoring high-velocity data streams to find operational anomalies. An Adaptive system's protocol modifies IoT defenses in response to the detected anomalies. Boosting the flexibility of IoT threat adaptation is why this system is most advanced. Streams of permanent and immutable data serve as the channels of communication among the IoT devices, and the data's integrity and authenticity are guaranteed by the decentralized ledger, which is also unchangeable. By allowing the framework to automatically perform defined actions when threats are detected, smart contracts further reduce the time systems are left vulnerable to adaptive malicious attacks.

This also fosters a collaborative environment among different stakeholders aimed at the same goals in efficient threat detection and response [4].

2. LITERATURE REVIEW

2.1 Current methods in IoT security

Security risks that are presented by the IoT come from its complex interlinkage of devices. The traditional defense mechanisms, especially intrusion detection systems (IDS) based systems, are not able to address the challenges provided by IoT interfaces, especially in environments where signature-based detection systems are the only option, since the evolving cyber threats cannot be neutralized. This has compelled the shift towards machine learning (ML) based anomaly detection, where the system is trained to flag behavior that is considered unusual for possible attacks. The advancements captured in DL recently offer increased promise value towards better threat detection of IoT systems by processing large streams of data instantaneously for rapid threat detection. Also, collaborative intrusion detection with data privacy breach of various IoT devices is being looked into with the help of federated learning. Table 1 shows an analysis of existing studies on operative threat intelligence for enhanced security aimed at IoT security enhancement.

Blockchain technology is also gaining attention as a means to enhance data integrity and secure communications within IoT frameworks by creating immutable transaction records, thereby addressing concerns related to data manipulation and unauthorized access. Collectively, these innovative strategies aim to develop stronger security architectures for IoT applications [4-6].

Table 1. A critical comparative analysis of existing studies on operative threat intelligence for enhanced security aimed at IoT security enhancement

Ref.	Key Contributions	Methodology/Framework	Main Findings
Saxena and Gayathri [7]	Identified CTI data sharing issues and proposed the CCTI system utilizing AI-based classification and blockchain immutability.	Execution of AI computations on blockchain platforms.	This study identifies CTI challenges and proposes a collaborative framework for secure threat information sharing.
Sarhan et al. [8]	Introduced HBFL: A privacy-preserving IDS using federated learning and decentralized blockchain storage.	Implementing hierarchical federated learning over blockchain infrastructure.	Privacy-preserving and secure intrusion detection in collaborative IoT environments. Demonstrated feasibility with evaluation and implementation using a key IoT dataset.
Arshad et al. [9]	Proposed COLIDE framework enabling energy-efficient detection via cooperative communication between border and sensor nodes.	Facilitated collaboration among border nodes and resource-constrained sensors.	Efficient intrusion detection in IoT systems with collaboration. Implementation and experimentation using Contiki OS demonstrated effectiveness with respect to energy and processing overheads.
Sarhan et al. [10]	Developed a federated learning scheme supporting CTI sharing with uniform data structures, enabling cross-organization ML training.	Leveraged a common data format and federated learning.	By employing an efficient ML-based architecture that removes the need for inter-organizational data exchange, the system was evaluated using NetFlow datasets and demonstrated accurate classification of diverse traffic types.
Kumar et al. [11]	Proposed the P2TIF framework, integrating scalable blockchain with CNN-based analytics to secure IIoT data sharing.	Combining DL modules and a scalable blockchain.	Validation on the ToN-IoT and IoT-Botnet datasets demonstrated that the proposed solution, which addresses security, privacy, and scalability challenges in IIoT, achieves high efficiency and scalability.
Our Study	Designed an end-to-end AI-enhanced CTI framework combining user reporting, blockchain immutability, and ML-based classification.	Underpinned by blockchain-secured data sharing, the framework integrates human expertise with ML-driven analysis.	This work addresses a research gap by presenting a comprehensive synthesis of collaborative threat intelligence approaches for IoT security.

2.2 Role of AI in threat detection

AI is improving the way we detect threats in IoT security frameworks. Cyber threats have changed, and traditional security techniques do not work and new threats require new measures. As illustrated in Figure 2, AI methods like DL and ML automate threat detection by reviewing and offline data from IoT devices and identifying patterns and threats during an attack. This allows threats and data breach risks to be mitigated quickly.

AI's contribution to IoT security helps to improve, adapt, and overcome. Security protocols in real time and on the fly to changes by threats and vulnerabilities. NLP helps by monitoring, reporting, and allowing humans to focus on critical tasks.

Neural networks in AI-driven IDS learn to distinguish the benign from the malicious actions in heterogeneous IoT environments. These systems do not have fixed sizes but are elastic to accommodate new attack patterns and a plethora of users.

Strengthening the security posture of IoT networks, organizations utilize AI to aid in the safeguarding of sensitive data to protect against unauthorized access or data breaches [12].

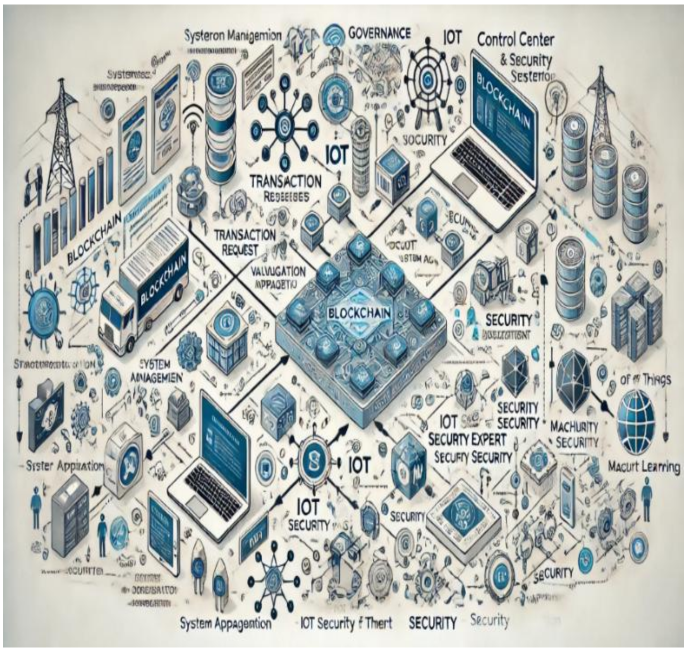


Figure 2. Integration of IoT, ML, and blockchain for enhanced security and transaction management

2.3 Application of blockchain in data integrity

The integration of IoT and blockchain increases the chance of a security breach and a cyber-attack focused on the blockchain technology that protects smart devices. As shown in Figure 3, blockchain can be integrated across the layered IoT architecture to secure identity, validate transactions, and preserve tamper-resistant logs of security events. At the center of this combination is a decentralized approach where every documented security breach is immutable and can only be verified by a full conspectus of the network. Hence, every piece of data is unalterable. It is this unalterable data that gives the security records their integrity. It is this raw, unmodified data that gives the security records their integrity and builds trust among the IoT stakeholders.

These participants will be able to share to improve security breach data triangulation in an ecosystem. With the adoption of blockchain technology, trust, transparency, and accountability can be brought to the system. The promising data on security breaches will be the driver for ML models to mature and be trained to predict unknown malicious threats. Furthermore, the blockchain's decentralized model provides stronger protection against potential cyber-attacks, as the absence of singular integration means there's no one point of failure.

Besides, the smart blockchain technology contracts have the capability to react on their own to threats by giving a fast mitigation of the attack. This reduces response lag and enhances the system's efficiency.

When integrated with the system, the surviving attributes and the AI algorithms with published threat detection capability, and the attacks in real time, passive to cyber threats to the integrity and confidentiality of the data, facilitates a more robust data defense system in place and in real time, the attributes [13].

To clarify how blockchain supports the proposed IoT security framework, the main benefits and their security implications are summarized in Table 2.

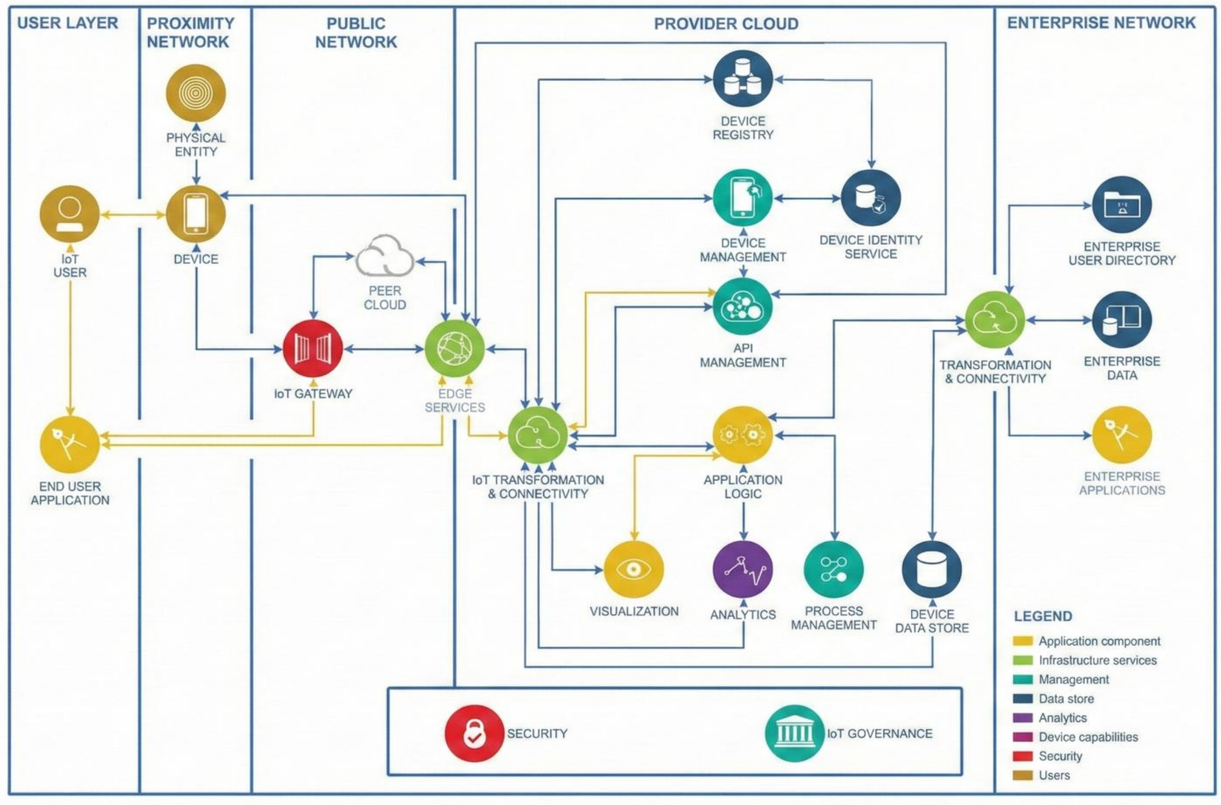


Figure 3. IoT system architecture

Table 2. Key blockchain contributions to integrity, trust, and automated response in the IoT security framework

Blockchain Benefits in IoT Security	Description
Immutability and Data Integrity	By guaranteeing data immutability and integrity, blockchain technology prevents unauthorized modifications or deletions, thereby ensuring the security incident records.
Transparency and Trust	Blockchain's decentralized, transparent ledger cultivates trust among IoT stakeholders by enabling all participants to access and verify security incident information, thereby promoting transparency and accountability.
Security Incident History	By maintaining a comprehensive history of security incidents alongside expert validations, blockchain provides the essential data needed for effective threat detection and trend analysis.
Decentralization and Resilience	Leveraging a decentralized blockchain architecture enhances system resilience by eliminating single points of failure; consequently, even if individual nodes are compromised, the blockchain's overall integrity is preserved.
Smart Contracts for Automation	Blockchain platforms' support for smart contracts facilitates automated security incident responses, thereby improving response times and overall system efficiency.

3. FRAMEWORK DESIGN

3.1 Architecture of the proposed framework

An incorporated architectural framework combining AI with blockchain was used to analyze the cybersecurity issues seen within IoT systems. The framework demonstrates the integration of a multi-tiered structure with AI-enabled cyber threat identification and the storage abilities of blockchain. The first layer consists of the IoT edge devices that send and receive data while communicating over a network. The next layer contains the algorithm-based AIs, such as ML and DL, which monitor the data streams for possible attack vectors.

Figure 4 demonstrates the interaction and data flow within the layers of the proposed framework that adheres to a defined three-layer design: the perception layer (sensing devices), the network layer (data transfer and blockchain record-keeping), and the application layer (AI-driven threat analysis). The data generated by IoT sensors positioned in the perception layer is transferred to the network layer that utilizes blockchain technology to ensure that the recorded data is immutable. The application layer then uses ML models to further analyze the validated data to detect and classify different types of cyber-attacks. The system also uses data captured from the application layer to change the rules of detection, allowing the system to modify itself in real time and assist in the further evolution of the system.

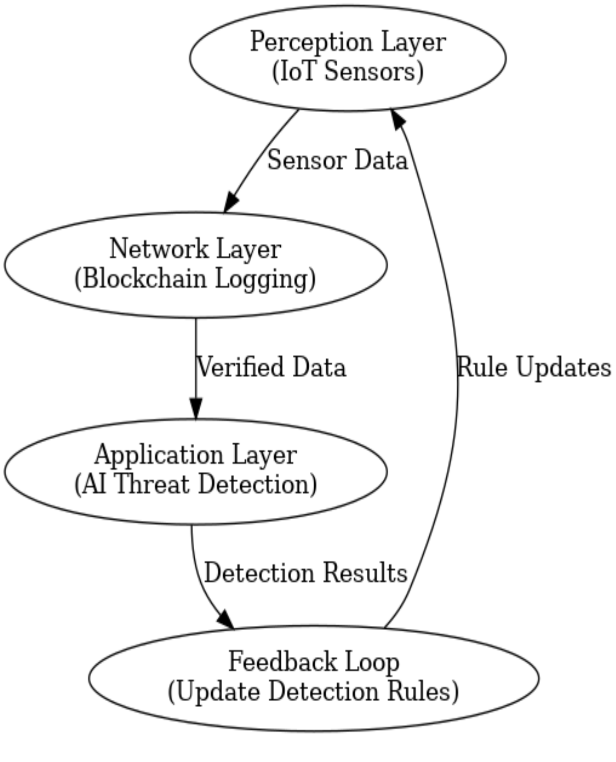


Figure 4. Interaction and data flow between layers

The fourth layer of the core of the blockchain contains cyber threat intelligence that is provably immutable in the fourth layer of the core of the blockchain. Here lies the transparency and the accountability of the interaction of the devices. Thus, in this case, the absence of detours to the central authorities is a good thing concerning the trust in the data that has been secured and encrypted. The fact that all the interactions that happen on the blockchain are systematically and provably time-stamped creates trust within the system.

In addition, the AI system's live alerts are posted publicly using a graphical interface to enable rapid human or automated responses from security teams. By combining AI's predictive power for finding abnormalities with the secure data management principles that blockchain provides, this model creates a powerful system that is not only resistant to threats that exist today but can also evolve to challenge security in the IoT world, both now and in the future [14].

To position the proposed framework within recent IoT security research, Table 3 summarizes representative studies that employ ML, blockchain, and mobile/iOS-oriented applications in different combinations.

Table 3. An analysis of research initiatives in IoT security: iOS applications, blockchain, and Emphasizing ML

Ref.	Blockchain	ML	iOS Application
[15]		✓	
[16]			✓
[17]		✓	
[18]	✓		
[19]		✓	
[20]		✓	
[21]	✓		
[22]	✓		
[23]	✓		
[24]	✓	✓	
[25]			✓
[26]			
[27]			
[28]			
This study	✓	✓	✓

3.2 Components involved: AI, blockchain, DL

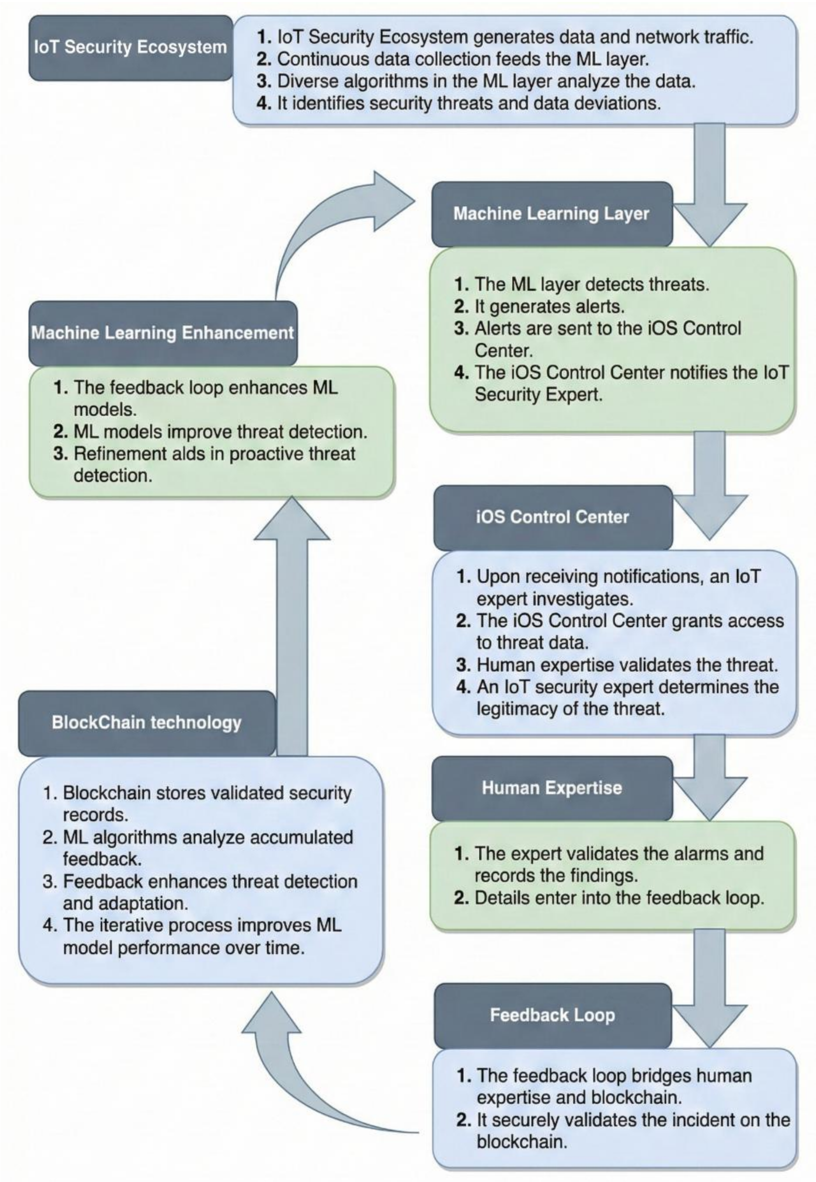
Integration of AI, blockchain, and DL technologies is crucial to IoT security expansion. AI helps with automated threat detection by providing algorithms that analyze data traffic and look for signs of a breach, such as unusual whirs. The prediction becomes more accurate as the system adapts using ML.

With IoT devices facing the throttle of the 'black box' issue of AI, blockchain will be the gatekeeper, the security incident logging ledger of AI. Its decentralized structure ensures that data will remain immutable since there is a low possibility of hacking and tampering. It takes user trust to the next level and does it without creating friction in data sharing in IoT.

Neural nets are the tools AI uses to process data, which is essential for a development running into action needing immediate attention, and for this, DL comes to the rescue. The framework is therefore significantly more secure thanks to the use of these three technologies that not only boost the violation detection rate but also reduce the number of times violations are responded to by mistake. These technologies provided a foolproof solution by not establishing an IoT system security hole [13].

3.3 Synergy between technologies for enhanced security

AI and blockchain together can advance the level of protection offered in IoT ecosystems. On one side, AI systems analyze large volumes of device and network data to detect trends and anomalies across the attack surface and support (near) real-time reaction. On the other side, blockchain stores identities, transactions, and security-relevant events in a decentralized and immutable ledger. In this way, when suspicious activities are flagged by AI, they are backed by a trustworthy record that cannot be altered after validation. This interaction and feedback-driven data flow is summarized in Figure 5.



1. IoT Security Ecosystem generates data and network traffic.
2. Continuous data collection feeds the ML layer.
3. Diverse algorithms in the ML layer analyze the data.
4. It identifies security threats and data deviations.

1. The ML layer detects threats.
2. It generates alerts.
3. Alerts are sent to the iOS Control Center.
4. The iOS Control Center notifies the IoT Security Expert.

1. Upon receiving notifications, an IoT expert investigates.
2. The iOS Control Center grants access to threat data.
3. Human expertise validates the threat.
4. An IoT security expert determines the legitimacy of the threat.

1. The expert validates the alarms and records the findings.
2. Details enter into the feedback loop.

1. The feedback loop bridges human expertise and blockchain.
2. It securely validates the incident on the blockchain.

1. Blockchain stores validated security records.
2. ML algorithms analyze accumulated feedback.
3. Feedback enhances threat detection and adaptation.
4. The iterative process improves ML model performance over time.

1. The feedback loop enhances ML models.
2. ML models improve threat detection.
3. Refinement alds in proactive threat detection.

Figure 5. Data flow within the IoT security framework

In the framework, the blended AI models are not fixed. They continue to learn from the past. Information about events detected by the model is recorded on the blockchain and subsequently used within a learning cycle. Over the course of many iterations, this logging and retraining will fine-tune the models to identify atypical and suspicious actions with increasing precision. The instantiation of this feedback cycle, along with real-time surveillance and semi-automated reaction to events, allows the system to close the gap on its defenses more quickly in response to an observed threat rather than waiting on a human operator for every single event.

From a broader view, AI and blockchain operate as one connected safety layer rather than two separate tools. AI improves threat recognition and prioritization, while blockchain helps preserve the integrity of the underlying data and maintains a traceable history of response actions with timestamps. Because these actions are stored on an immutable ledger, they can later be reviewed and audited, supporting accountability and more reliable post-incident analysis. In practical terms, this setup reduces average response time and strengthens the resilience of IoT infrastructures against persistent and evolving threats [29].

4. METHODOLOGY

4.1 Data collection and preprocessing techniques

In any AI-driven IoT security system, a system needs to be created to manage and control data from various sources. These sources include IoT devices, gateways, and networks, which all produce data in the form of system and user logs and network traffic. These data sources continually produce information and need to be controlled for effectiveness. Streams of information need to be captured in a fashion so they can be logs that are useful for later analysis, and not be logs that are unusable.

Once a system to control the data streams is complete, the information captured rarely arrives as a digital fingerprint. In order to prep the information, a phase needs to occur to improve data quality, and information is corrected, duplicate entries are erased, and missing values are dealt with as best as possible. In order to prep the data for the ML algorithms to be fair, the information needs to be normalized in order to reduce bias. Feature selection is also used in order to determine which values are useful to classify data. In ML, poorly performing features can often lead to the training process of different models being baffled.

When real-time streams are added into the pipeline, another difficulty appears: the volume of incoming information. In such cases, effective filtering techniques are required to strip out redundant or irrelevant records before deeper analytics are applied. This step prevents the models from being overwhelmed while still preserving enough context to build a robust dataset that can support accurate threat detection by advanced AI algorithms [30].

Privacy compliance in data collection. In scenarios involving sensitive information—especially healthcare data—privacy concerns become central rather than secondary. In this study, all data were anonymized before any analysis took place. Personally identifiable information (PII) was removed or masked using hashing and related techniques, and the datasets were either obtained from public sources or generated synthetically to avoid direct exposure of real patients. The collection and processing procedures followed key principles inspired by regulations such as HIPAA and GDPR, so that no individual's sensitive health information could be traced back, leaked, or misused during model training and evaluation.

4.2 Development of DL models for threat detection

Modern IoT environments are complex and advanced, and require more than simple signature-based and rule-based approaches to capture all informing security threats. To capture all informing security threats, DL models are used to learn what typical activity looks like and point out anomalies that could suggest illegal entry. These models have been used on both supervised and unsupervised learning to differentiate between legitimate network traffic and suspicious activity on network flow and device logs. Particularly, when input is treated as spatial patterns, convolutional neural networks (CNNs) are very useful. Also, recurrent neural networks (RNNs) as well as other architectures are very useful for temporal sequences like video, audio, or other events that have been time-stamped.

When several devices or organizations cooperate on training a joint model while keeping their raw data private, Federated Learning introduces an additional complementary strategy. Local model parameters are updated, and only aggregated updates are sent, ensuring stronger privacy while still advancing detection. Popular DL frameworks like TensorFlow and PyTorch are customizable and offer modular parts that facilitate developing models specific to different IoT devices and/or use cases that have different hardware constraints and vary in workloads and latency needs.

Among all these methods, the detection of abnormalities among the normal behavior patterns remains the primary focus. Ensemble methods help in improving the reliability of the solution by aggregating the outputs/probabilities of different models. For example, if one model misclassifies a given pattern, the collection of other models could still detect the pattern in question, ultimately providing a more reliable prediction in the final answer. Experimental studies in the literature show that such DL-based and ensemble techniques often reach state-of-the-art accuracy in threat detection and outperform traditional rule-based mechanisms by a noticeable margin. Furthermore, optimization steps such as careful hyperparameter tuning, model regularization, and architecture search can further refine performance, especially when real-time threat hunting is required in live IoT deployments [6, 31].

4.3 Implementation of blockchain for data integrity

To complement the learning capabilities of AI, blockchain is integrated into the framework as a mechanism for preserving data integrity and providing an auditable history of security-relevant events. A private or permissioned blockchain is adopted so that participation and access rights can be aligned with the security requirements of the specific IoT environment. Because entries on the ledger are immutable once confirmed, attempts to alter or falsify recorded information can be detected, which is particularly important when sensor readings or logs might be targeted by attackers. The main blockchain protocols and the key features that support IoT integrity are summarized in Figure 6.

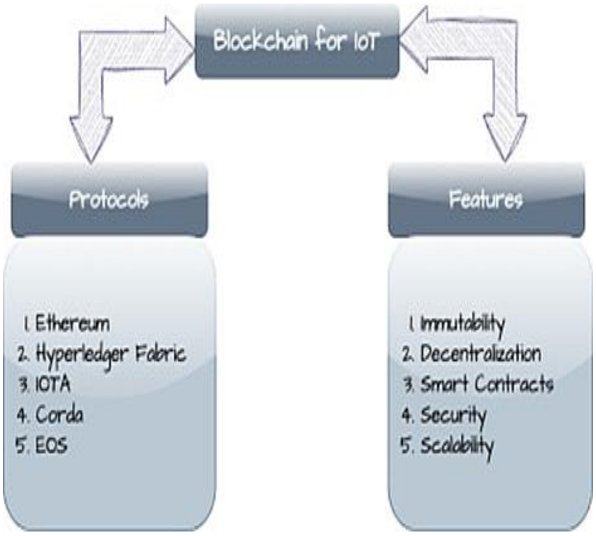


Figure 6. Blockchain for IoT, protocols, and features

Smart contracts can help automate rule enforcement concerning when and how to log threat detection, flushing out response workflows, and ensuring consistent logging of detection results. They sit at the top of the ledger and help in the key verification and feedback center process. Along with these, additional safeguards to address data confidentiality and protection include digital signatures and other forms of cryptographic network protection. Only those with the appropriate access may view, modify, or annotate sensitive information, and these cryptographic protective devices allow their movement across the network.

Trust with data storage and the decentralized framework of a blockchain allows the framework to sidestep the problem of a single point of failure. Each logged event and associated data is time-stamped and cryptographically linked to all previous data, ensuring a single secure path for all future data to be added. This framework will integrate with other IoT devices to enable rapid response and threat mitigation, and will also support the assurance of data accuracy and provenance across all connected devices [4].

5. EXPERIMENTAL SETUP AND TESTING

5.1 Test environments: IoT settings vs. healthcare settings

In this part, we continue by looking more closely at the test environments that were set up to validate the proposed AI-blockchain security framework. The goal was to see how the framework behaves in two different worlds: a general IoT environment on one side, and a healthcare-focused IoT environment on the other. In a typical IoT setting, there are many interconnected devices producing continuous streams of data. Every individual device has unique security challenges, as the biggest concern remains keeping communication secure, keeping data protected, and maintaining data integrity while everything is simultaneously online and vulnerable to cyber-attacks. Within this context, the scope of hypothetical tests of this problem is likely to include deliberate attempts to gain unauthorized access, attempts to introduce malicious data, and cases where attempts at intrusion might fall under the detection gap.

The challenges brought by the healthcare field are even more prominent as the data in question is no longer just technical data, but data about patients and their conditions. As a result, privacy becomes a non-negotiable given alongside compliance with relevant legislation such as HIPAA. Any AI-based mechanism has to analyze the data in real-time while maintaining the utmost confidentiality. In this case, the use of Blockchain technology to store Electronic Health Records and ensure that only relevant personnel are granted access in real-time during the processing of sensitive data is of great importance.

Two kinds of environments were simulated to check the adaptability of the framework to varying levels of security and sensitivity of the data [32, 33]. Therefore, the experimental arrangement was divided into two cases. In the overall IoT case, the devices were ordinary smart sensors, smart devices in homes, and industrial controllers. The data amounts were of moderate size, and the primary security concern was the integrity of the devices and control of network access by selective downstream control. In the case of IoT in the Healthcare environment, the devices included medical sensors, wearables for remote monitoring, and data gateways for capturing patients' data. This second environment dealt with larger volumes of much more sensitive data and had to implement stronger safeguards to meet real-time anomaly detection, end-to-end encryption of data in transit, and healthcare data privacy compliance. Testers understood these considerations, and the resulting balance in constancy and variability compared across the two domains was the result of this being a case of true, and not artificial, testing.

5.2 Performance metrics for evaluation

In order to evaluate the effectiveness of the AI blockchain framework performance, the application of particular standardized metrics will be considered. The metrics under consideration include: accuracy, precision, recall, F1-score, and area under the ROC curve (ROC AUC). Each of these metrics describes particular characteristics of the detection model's behavior. Accuracy describes the overall picture of how many instances (both attacks and normal events) are correctly classified. Precision describes the subset of alerts that the model predicts to be threats and asks the question: how many of those are truly malicious? A high precision indicates that there are fewer false alarms.

In contrast, recall answers the question: how many of the actual threats that are present in the data set did the model capture? A low recall indicates that there are dangerous events that the model is missing. Because precision and recall can move in opposite directions, the F1-score calculates them into a single value, which is useful in scenarios where the dataset is skewed, which is common in the IoT, where real attacks are much less frequent than regular activities.

In order to have a complete analysis, we look at the ROC-AUC metric. The ROC curve shows the relation of true positives to false positives at the different levels of a decision. The area of the curve shows the model's ability to determine benign and malicious actions at varying levels of the metric. Considering all of these metrics explains in a more complete manner the framework's suitability for real-time threat detection.

Practical considerations must also be incorporated beyond the classification's quality. These practical considerations include the model's answering speed, the consumption of resources, and its execution efficiency depending on the workload. The aim is to show the model's ability to detect threats in a precise manner while also proving the model's suitability for use in real IoT and healthcare environments, with acceptable response times and costs [13, 32].

5.3 Tools and technologies used in the testing phase

Evaluating the advantage of this potential framework was done through various means of tools and techniques. The implementation of IoT devices into healthcare systems facilitated the collection of device-anchored usage and network communication data in real-time, which is crucial in adapting the system performance to various conditions.

Equally applicable to the case were techniques like preprocessing, normalization and the filtering of noise signals from the data, which smoothen the data for entry to the DL algorithms. Threat detection DL models were developed with TensorFlow and Keras, being a high-level TensorFlow API which facilitates the building and training of neural networks.

Moreover, during the testing phase of the solution, blockchain technology was introduced to ensure the integrity of the data. Event logging and all interactions between IoT devices were secured through private blockchain protocols to prevent unauthorized access. Four applications have been investigated and developed on Ethereum and Hyperledger Fabric with the purpose of creating decentralized applications that meet the framework's security requirements. This will allow outlining the principal concept behind innovative works on possible approaches on how AI can be integrated with blockchain technology to improve security inside IoT, and which methods have been taken among others [32, 33].

6. RESULTS AND DISCUSSION

6.1 Effectiveness of the AI-driven model in detecting threats

IoT threat detection model (AI-powered): The proposed model shows strong capability in classifying IoT threats with high accuracy. It relies on ML and DL techniques, including decision trees and neural networks, to analyze large volumes of IoT data and identify irregular behavioral patterns that may indicate security incidents. In practical testing, DL-based methods are particularly useful for capturing subtle anomalies that can be missed by traditional rule-based systems, especially in dynamic IoT environments. The main features and expected advantages of the proposed framework are summarized in Figure 7.

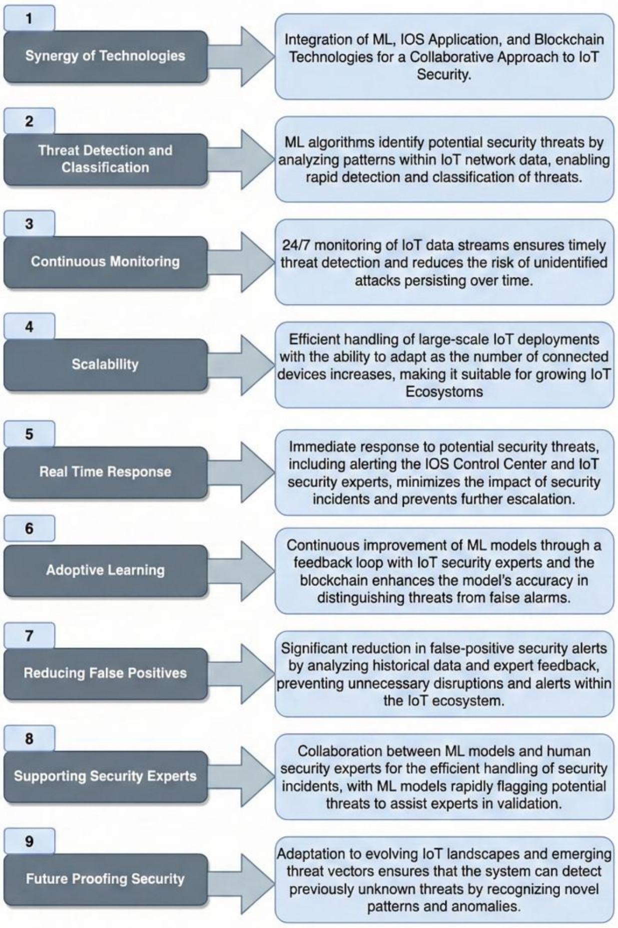

1
Synergy of Technologies
Integration of ML, IOS Application, and Blockchain Technologies for a Collaborative Approach to IoT Security.
2
Threat Detection and Classification
ML algorithms identify potential security threats by analyzing patterns within IoT network data, enabling rapid detection and classification of threats.
3
Continuous Monitoring
24/7 monitoring of IoT data streams ensures timely threat detection and reduces the risk of unidentified attacks persisting over time.
4
Scalability
Efficient handling of large-scale IoT deployments with the ability to adapt as the number of connected devices increases, making it suitable for growing IoT Ecosystoms
5
Real Time Response
Immediate response to potential security threats, including alerting the IOS Control Center and IoT security experts, minimizes the impact of security incidents and prevents further escalation.
6
Adoptive Learning
Continuous improvement of ML models through a feedback loop with IoT security experts and the blockchain enhances the model's accuracy in distinguishing threats from false alarms.
7
Reducing False Positives
Significant reduction in false-positive security alerts by analyzing historical data and expert feedback, preventing unnecessary disruptions and alerts within the IoT ecosystem.
8
Supporting Security Experts
Collaboration between ML models and human security experts for the efficient handling of security incidents, with ML models rapidly flagging potential threats to assist experts in validation.
9
Future Proofing Security
Adaptation to evolving IoT landscapes and emerging threat vectors ensures that the system can detect previously unknown threats by recognizing novel patterns and anomalies.

Figure 7. Features of the proposed framework

To develop a model in a more comprehensive manner, a blockchain technology layer is added in order to link data integrity to a permanent record of a security event's details. In other words, the AI is not just anomaly detection, but also works with a ledger that records every attack and every countermeasure taken against that attack. A logging and anomaly detection cycle is created so the information inscribed on the ledger can be recycled to retrain the ML models, improving detection efficacy and reducing false positives over time.

Such a model, especially in highly challenging areas like healthcare, is expected to outperform actioners of ML, particularly SVM and KNN, on various dimensions, including, but not limited to, precision, recall, interpretability, and F1. The indifferent model, Latin other data comes in, is able to gain increments while the blockchain stores expert annotations on the anomalous events that constitute an empirical country to the system. Ultimately, the integrated system is able to more accurately task genuine anomalies and harmless threats, while moving in the complex real world [6, 34].

6.2 Impact of blockchain on data integrity during attacks

Developments of trust management have seen blockchain software engineers build cross-disciplinary, integrated IoT blockchain applications. In IoT blockchain applications, the most significant feature is the management of evidence of the attack. With interlinked blocks, significant events are recorded in a way that is difficult to modify without detection. It produces a sequence of events detailing the attacks, breaches, and responses that are permanently available to attack, vary, or shut down the attack. In defending the domain, trusted consecutive events record a precise approximation of the events, enhancing security for `tethered dumping` of sensor logs or evidence of the network.

The ledger's consistency is protected due to the lack of single points of failure, and smart contracts support the integrity of the shared security view. Decentralization contributes even more to this protection. Compromising a few of the nodes does not disrupt the ledger's consistency. Trigger workflows and automated responses to validated alerts issued to suspicious events. Access restrictions and responsiveness are supported to further mitigate the time it takes to fully respond to the situation. Overall, organizations are under constant evolving attacks and are focused on IoT security, separating blockchain from an operational form of security. Increasingly useful and reliable defense should be the goal of organizations and attack conditions [2, 13].

To provide a broader view of how blockchain has been integrated with IoT across different application domains—along with the main benefits and recurring limitations reported in the literature—the key representative studies are summarized in Table 4.

Table 4. A review of the integration of IoT and blockchain across various domains

Ref. No.	Focus	Advantages	Limitations
Dorri et al. [35]	Improving blockchain to support IoT.	Enhancing blockchain technology to facilitate efficient, cost-effective deployment in IoT applications.	Trade-off between scalability and security, with potential for vulnerabilities inherent to the consensus mechanisms underpinning the system.
Novo [36]	Hybrid blockchain architecture for IoT.	Scalable and decentralized infrastructure for secure data exchange in IoT networks.	The adoption of blockchain introduces greater complexity compared to conventional architectures and may result in scalability bottlenecks under high transaction loads.
Fernández-Caramés and Fraga-Lamas [37]	Ensuring dependable IoT infrastructures through the integration of blockchain technology.	Utilizing blockchain to improve fault tolerance and ensure data integrity in IoT systems.	Scalability challenges and potential for network congestion as the number of devices increases.
Dutta et al. [38]	Benefits of blockchain in the supply chain.	Enhancing transparency, reducing fraud, and ensuring traceability in supply chain management with blockchain.	Integration challenges between existing systems and potential privacy concerns regarding data visibility.
Tian [39]	Leveraging blockchain and IoT in SCM.	Combining IoT and blockchain to improve and reduce costs and supply chain visibility.	Increased complexity in implementation and potential interoperability issues between different systems.
Khan and Salah [40]	Function of blockchain in IoT.	Utilizing blockchain technology for maintaining data integrity, transparency, and decentralized control in IoT systems.	Potential scalability limitations and increased energy consumption compared to centralized approaches.
Khrais [41]	Function of blockchain and IoT in a smart city.	Utilizing IoT and blockchain to improve efficiency and enhance data security in smart city applications.	Integration challenges between various systems and potential privacy concerns regarding collected data.
Atlam and Wills [42]	Blockchain framework for IoT.	Developing a blockchain framework for reliable data management and security in IoT networks.	Scalability limitations and potential performance bottlenecks as the network grows.
Azaria et al. [43]	Monitoring and securing healthcare data.	Enabling tamper-proof healthcare data records and enhanced security through blockchain technology.	Privacy concerns regarding potential regulatory hurdles and sensitive health data in healthcare data management.
Balhareth et al. [44]	Security perspective of IoT integration.	Enhancing data security and reducing fraud risk through blockchain integration with IoT systems.	Increased potential performance overhead and complexity due to the blockchain's distributed nature.
Ahad et al. [45]	Blockchain, IoT, and 5G in smart healthcare.	Leveraging the combined benefits of blockchain, 5G technology, and IoT to improve privacy and security in smart healthcare systems.	Integration challenges between these disparate technologies and potential scalability issues.
Ferrag et al. [46]	Security issues and privacy in blockchain-based IoT systems.	Identifying and addressing privacy and security vulnerabilities in blockchain-based IoT systems.	Balancing privacy concerns with the need for data transparency and potential security exploits in the underlying blockchain technology.
Fromhart and Therattil [47]	Loyalty management systems powered by blockchain.	Utilizing blockchain to reduce costs and incentivize customer loyalty in loyalty programs.	Requirement for a generic platform to address potential integration challenges and facilitate widespread adoption with existing systems.
Jafar et al. [48]	Verifiability and privacy in e-voting.	Achieving both verifiability and privacy in electronic voting systems using cryptographic primitives enabled by blockchain.	Increased complexity due to potential usability challenges and cryptographic techniques for voters.
Atlam et al. [49]	Examination of IoT applications and privacy/security concerns.	Analyzing privacy and security risks associated with various IoT applications and proposing scalable.	Difficulty in implementing effective solutions and adapting existing policy frameworks to address the evolving nature of IoT threats.
Wang et al. [50]	Revolutionizing healthcare data sharing using a secure hybrid blockchain approach.	Unlocking the power of secure and private health data exchange.	Navigating the intricacies: Implementation complexity and potential scalability hurdles.

In all fields considered, while supporting integrity and traceability, blockchain consistently experiences limitations with scalability, interoperability, and deployment complexities.

6.3 Comparative analysis between traditional methods and proposed framework results

Traditional IoT security still depends largely on centralized or semi-centralized controls such as firewalls, segmented access rules, and static policy enforcement. These measures are useful in controlled settings or against straightforward attacks, but they often struggle when threats become distributed, coordinated, or adaptive across a large number of connected nodes. In such cases, the security system may detect events but still lack reliable, tamper-resistant records that preserve what actually happened. This is where blockchain can add practical value by providing immutable logging and stronger trust in incident records, rather than relying only on conventional device-centric defenses.

From the ML side, classical baselines such as SVM and

KNN can deliver reasonable performance on certain traffic patterns. CNN-based detection can also be effective, particularly when data representation supports deep pattern extraction. However, performance stability becomes more challenging as the deployment scale grows and the number of nodes increases. The proposed BBMDA-based framework appears more consistent under these conditions, especially when the environment is larger and more dynamic.

As shown in Figure 8, BBMDA achieves the highest accuracy across all tested node settings (from 10 to 100 nodes) compared with SVM, KNN, and CNN. The gap becomes more noticeable at higher node counts, which suggests that the proposed structure handles scale-related complexity better than the baseline methods. This trend supports the idea that combining advanced ML with a blockchain-backed integrity layer can improve not only detection outcomes but also the trustworthiness of the recorded results.

In addition, retaining security-relevant actions and authentication events on an immutable ledger provides a clearer audit trail during or after an attack. This is particularly important in sensitive IoT domains, where incident investigation requires reliable evidence and consistent event reconstruction.

There are positive aspects to deployment, but there are still financial and operational restrictions to consider. In tandem with all of the blockchain infrastructure, deep models running would require additional computational and storage resources, and complications may arise from trying to fit it to existing structures. These challenges may be more pronounced in healthcare-oriented IoT environments due to the volume and sensitivity of data. Still, the performance gains and enhanced accountability offered by the framework can justify the added complexity in scenarios where trust, integrity, and fast detection are critical

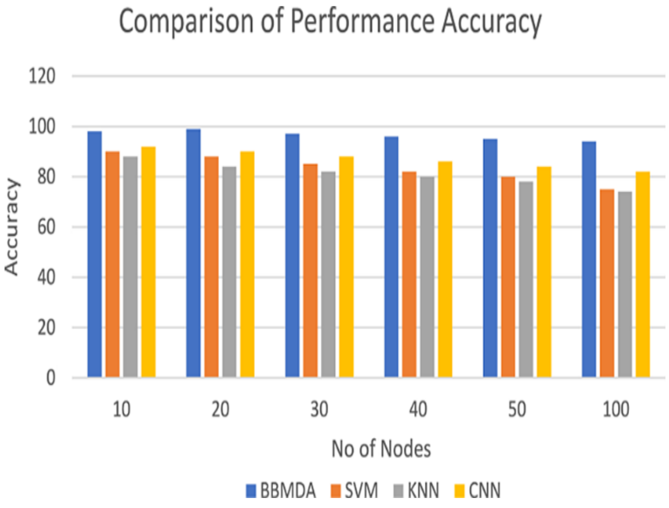


Figure 8. Full-size image of the proposed BBMDA model accuracy

7. CASE STUDIES: APPLICATIONS IN REAL-WORLD SCENARIOS

7.1 Security threats faced in IoT environments

IoT ecosystems have various security issues ecosystems that impact both the service and security of the ecosystems. The most simple and critical of these issues is the fact that many of these devices have lower than normal security and can be subjected to data breaches, cyber incidents, and intrusions. Because these systems are typically built as distributed architectures, they increase the surface of the attachable area. Malicious users can exploit weak authentication and default passwords. Common examples of this are DDoS attacks, where a significant number of compromised devices are used as bots to send superfluous traffic to the targeted network, and man-in-the-middle attacks, where an adversary discretely intrudes to alter the data that is released between the systems.

A great number of IoT devices and sensors are also afflicted with the same problem of low processing power and memory. This makes it hard for such end devices to implement strong encryption and robust security measures, and thus, they are more vulnerable to a wider scope of attacks. The impact of such frailties becomes especially glaring in certain sectors like healthcare and industrial control, where one mistake or instance of malpractice can be catastrophic and, in some cases, fatal.

An adversary targeting a single network protocol might be able to modify or remove critical data. In addition, gaining physical access to a device might be sufficient to obtain or obliterate extremely confidential data saved on the device as well.

These compound challenges go on to call for security solutions capable of addressing both present and future threats, while still enabling trust among the various IoT ecosystem constituent parts [4, 31, 51, 52].

7.2 Case study for healthcare security

Various industries use the IoT at different levels, but the healthcare sector is particularly susceptible to cyberattacks because most IoT devices deal with sensitive patient data. A framework for supporting medical IoT devices based on AI and a blockchain-based healthcare model. Utilis' data breach prevention AI algorithm detects anomalies and predictive analytics instantly, allowing the security team to identify threats like unusual access to electronic health records.

This enhanced security would be inaccessible through any other method because the data would be protected at the source, and priority filtering would be executed using smart contracts on the blockchain to allow regulated and secure access to patient information. This protects you from unauthorized access and, due to that, maintains a high level of trust among the patients and the healthcare professionals.

This case study underlines the significance of blockchain in protecting the integrity of medical information from a cyberattack. The system's resistance to corruption is based on decentralization; when health record storage is decentralized, even if one node is compromised, others are not. AI and blockchain together provide a strong basis that helps prevent security breaches and boosts the operations in healthcare [33, 53].

7.3 Advantages received from instituting the framework

The implementation of the suggested security framework is a great step towards improving the security of the IoT system since it utilizes AI and blockchain technology. The first of these is the removal of integrated mobile payment systems and accompanying apps on the provider's website.

Even if we ignore the costs of removing the apps, high ongoing costs must be incurred. For example, ongoing software maintenance, especially with platform migration and upgrades, and ongoing predictive analytics and reporting must be performed. Even ignoring costs incurred by maintaining the apps, these costs must be incurred. Analytical costs must be incurred not as self-assigning tools, but to determine value-added savings and efficiencies to be derived through the app.

The ongoing costs incurred through the targeted analytics must not be self-assigning in nature. They must be genuinely targeted towards the costs of the apps and associated efficiencies in service delivery, or focused on determining savings and efficiencies to be derived from the removal of the apps.

In conclusion, if the integrated mobile payments and apps were removed from the online systems, high average costs would be incurred by removing the systems, and the ongoing predictive costs would be deeply incurred through the analytical system built on self-assigning attributes, which wouldn't be acceptable.

In summary, integrated mobile payment systems can significantly worsen the overall analytics system, especially predictive analytics systems, to a great degree. It is in the best interest of the provider to remove those integrated mobile payment systems. Thus, it was shown that by combining the actual benefits of SIEM and SOAR, one can achieve better operational efficiency through automated threat responses alongside incident management processes [4, 51].

8. LIMITATIONS AND CHALLENGES

8.1 Challenges encountered during enactment

Bringing blockchain and AI together to secure IoT systems is promising, but it is far from straightforward. One of the main problems is the scalability of blockchain itself. As more and more devices connect to the network, the number of transactions that must be written and validated on the chain increases, which can slow down the processing rate. When this happens, it becomes harder to support near-real-time logging and detection of security events. At the same time, many modern AI models are large and complex, and they require significant computation and memory, which makes the combined setup even heavier to deploy.

Another difficulty comes from the IoT devices at the edge. Most of them were not designed to run heavy cryptography or DL; they have limited processing power, storage, and battery life. Complicated blockchain protocols or costly AI workflows would hit issues such as lag or interruptions, and there would be excessive battery drain. The performance and safety trade-off would need to be engineered to spend as little energy as spent, as little time is wasted, and energy is used to as little as possible. The trade-off to safety fundamentals here would be that large tasks can be offloaded to gateways or edge servers, rather than letting the sensor deal with them alone.

The intricate difficulty of gaining access to data can complicate things even further. For AI-based security to function correctly, it needs massive amounts of data to authenticate and test. This is especially true for personal and medical information, which is extremely sensitive. This doesn't make it easier to attempt using verifiable real-world datasets, and it may even act as a deterrent. Other options, like the generation of synthetic data or the use of extremely anonymized logs, may be needed to determine whether and to what extent the framework meets the required functioning. Furthermore, the cyber threat landscape is ever-changing. New attack models are introduced with alarming frequency, and changes to the models, rules, and security policies are required to be adaptive. Keeping layers of defenses both current and capable of pulling back the threat is an enduring challenge, and in most cases, the answer won't be as simple as 'just make a model and it will work [32, 51].

8.2 The evolution of IoT security and challenges ahead

The number of connected devices keeps growing, and so does the challenge of securing the IoT. Each of these devices can potentially be an attack vector. Today's IoT ecosystems also tend to be quite heterogeneous: there are different vendors, devices, platforms, and communication standards. The absence of a common standard means there is no way to implement a unified security strategy. then there are new, rapidly evolving technologies such as AI and blockchain. these add new systems and require ongoing oversight and adjustments, which tend to annoy people. the more systems there are to oversee, the more attackers will try to find and exploit weaknesses.

Another problem is the Privacy of the data, which is in many cases very sensitive. Examples of this are health data, localization data, and data on the metrics of a certain industrial process. Privacy concerns are a demand. The foremost concern is the need for the enactment of policies focused on Access Control, Strong Encryption, Privacy-Enhancing Technologies, and the minimization of harmful use of the user's data. The Interoperability Problems of disparate IoT systems, which undermine global Security, are cause for concern. The need for the development of Secure communication systems designed to be Interoperable is apparent. Standardized secure communication protocols will solve the diverse and interdependent nature of the problem.

Problems abound in the area of compliance with regulations too. Notably, the legal structure and the tech world do not move in synch, and in most instances, there is a disconnect between the legal frameworks and what is actually happening in the real world, giving rise to an absence of a legal approach to the integration of the new dimension of the IoT and AI-blockchain. It is extremely hard to conceptualize and articulate a plan to defend against cyber threats and simultaneously address the fundamental problems of privacy being used as a throttle to inhibit innovation. The right balance, if there is to be any, can be only achieved with the joint effort of the three stakeholders of the IoT ecosystems: the industry, the academia, and the policy makers, if the IoT of tomorrow is to be safe and sustainable [31, 33].

9. CONCLUSIONS AND FUTURE WORK

This synergy demonstrates how AI and Blockchain can be utilized together to enhance the IoT ecosystem's security. The strength of the proposed system is the amalgamation of the components of AI, which are the ability to detect threats and an adaptive real-time response to changing attack patterns, with the characteristics of Blockchain, which provide data integrity and transparency, and a verifiable trail of events. The AI system is capable of adapting to an attack and strengthening the defense system of the secured mechanism, while the Blockchain makes credible the information that was transmitted during the attack and ensures that the recorded events are valid.

The appraisal also indicates that the integrated DL model is better at complex pattern recognition as compared to homogeneous systems (IDS). This is particularly relevant in cases where confidentiality is pivotal, such as the healthcare industry. In such cases, the marginal cost of a false negative is high; thus, the additional accuracy brought in by the framework is of great importance. In totality, the blend of AI and Blockchain is a great improvement, and the analyzed case studies show the value of the approach in data protection, visibility of threats, and the safe disposal of classified data [2, 31, 34, 54].

That said, the framework possesses shortcomings and does not provide a complete solution to the problem at stake. In the case of massive IoT networks, containing thousands and tens of thousands of devices, scalability can represent a major challenge. If the system is not appropriately configured, there can be a negative impact on real-time operation due to transaction delays in the blockchain and the computational demands of the DL models. In addition, the current system design has a hypothesis of a stable correlation along with a minimum level of device tampering. These assumptions are not likely to be the case in highly flexible or severely restricted circumstances. These shortcomings point naturally to areas where future work can refine and extend the framework to make it more flexible, lighter, and better adapted to a wider range of IoT scenarios.

9.1 Recommendations for future enhancements to the framework

The ways the proposed AI-blockchain security framework can be improved must be in several different directions. One of the most important of these is integrating more sophisticated ML processes. The more sophisticated the ML processes are, the better they will be able to enhance the functioning of the blockchain in regard to the detection of incidents in real time, as well as the responses to such incidents. Predictably, the use of distributed or edge AI models would enhance the ability of the organization to perform security analytics more proximal to the point of data generation, while also preserving the majority of training data sequestered, thus not losing control over the data while avoiding sentry uploads to a primary server. Ideally, such systems would be more difficult to compromise while also providing more sophisticated responses in a timely manner to hostile activities.

An equally important field of study is user-centered security. If the interface, alerts, and the overall organization of data in the system are designed with the user and operator in mind, they can serve security management as an active counter and as a tool to better understand the discipline and mechanisms of the IoT, as opposed to a user simply functioning as an automatic decision endpoint. User-friendly, simple, and designed icons, dashboards, and status lamps on the control panel can elevate the security culture and make the user more sensitive to the system and active in responding to the system when problems arise. The large-scale expansion of the IoT intensifies the need for robust interoperability and seamless plug-and-play capabilities. Future research is likely to emphasize scalable Layer 1/Layer 2 blockchain infrastructures and lightweight decentralized consensus mechanisms tailored to IoT constraints. As blockchain ecosystems become increasingly heterogeneous, cross-chain interoperability will be essential to enable secure, low-latency event exchange across IoT domains. In parallel, effective deployment will require alignment between technological development, regulatory frameworks, and business strategies to support the integration of blockchain and AI in real-world IoT environments.

REFERENCES

[1] Antonakakis, M., April, T., Bailey, M., Bernhard, M., et al. (2017). Understanding the Mirai botnet. In 26th USENIX Security Symposium (USENIX Security 17), Vancouver, BC, Canada, pp. 1093-1110. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis.

[2] Ruzbahani, A.M. (2024). AI-protected blockchain-based IoT environments: Harnessing the future of network security and privacy. arXiv preprint arXiv:2405.13847. https://doi.org/10.48550/arXiv.2405.13847

[3] Azizah, D.M., Oktavia, C. (2024). Implementing blockchain technology for securing IOT-based smart grids. International Journal of Electrical Engineering, Mathematics and Computer Science, 1(1): 9-12. https://doi.org/10.62951/ijeemcs.v1i1.70

[4] Gopalan, S.H., Manikandan, A., Dharani, N.P., Sujatha, G. (2024). Enhancing IoT security: A blockchain-based mitigation framework for deauthentication attacks. International Journal of Networked and Distributed Computing, 12(2): 237-249. https://doi.org/10.1007/s44227-024-00029-w

[5] Waheed, N., He, X., Ikram, M., Usman, M., et al. (2021). Security and privacy in IoT using machine learning and blockchain: Threats and countermeasures. ACM Computing Surveys, 53(6): 122. https://doi.org/10.1145/3417987

[6] Aldhaheri, A., Alwahedi, F., Ferrag, M.A., Battah, A. (2024). Deep learning for cyber threat detection in IoT networks: A review. Internet of Things and Cyber-Physical Systems, 4: 110-128. https://doi.org/10.1016/j.iotcps.2023.09.003

[7] Saxena, R., Gayathri, E. (2022). Cyber threat intelligence challenges: Leveraging blockchain intelligence with possible solution. Materials Today: Proceedings, 51: 682-689. https://doi.org/10.1016/j.matpr.2021.06.204

[8] Sarhan, M., Lo, W.W., Layeghy, S., Portmann, M. (2022). HBFL: A hierarchical blockchain-based federated learning framework for collaborative IoT intrusion detection. Computers & Electrical Engineering, 103: 108379. https://doi.org/10.1016/j.compeleceng.2022.108379

[9] Arshad, J., Azad, M.A., Abdellatif, M.M., Ur Rehman, M.H., Salah, K. (2019). COLIDE: A collaborative intrusion detection framework for Internet of Things. IET Networks, 8(1): 3-14. https://doi.org/10.1049/iet-net.2018.5036

[10] Sarhan, M., Layeghy, S., Moustafa, N., Portmann, M.

(2023). Cyber threat intelligence sharing scheme based on federated learning for network intrusion detection. Journal of Network and Systems Management, 31: 3. https://doi.org/10.1007/s10922-022-09691-3

[11] Kumar, P., Kumar, R., Gupta, G.P., Tripathi, R., Srivastava, G. (2022). P2TIF: A blockchain and deep learning framework for privacy-preserved threat intelligence in industrial IoT. IEEE Transactions on Industrial Informatics, 18(9): 6358-6367. https://doi.org/10.1109/TII.2022.3142030

[12] Junaid, S.B., Imam, A.A., Balogun, A.O., De Silva, L.C., et al. (2022). Recent advancements in emerging technologies for healthcare management systems: A survey. Healthcare, 10(10): 1940. https://doi.org/10.3390/healthcare10101940

[13] Nazir, A., He, J., Zhu, N., Wajahat, A., et al. (2024). Collaborative threat intelligence: Enhancing IoT security through blockchain and machine learning integration. Journal of King Saud University-Computer and Information Sciences, 36(2): 101939. https://doi.org/10.1016/j.jksuci.2024.101939

[14] Khan, S., Khan, M., Khan, M.A., Khan, M.A., et al. (2025). A blockchain-enabled AI-driven secure searchable encryption framework for medical IoT systems. IEEE Journal of Biomedical and Health Informatics, 1-14. https://doi.org/10.1109/JBHI.2025.3538623

[15] Pan, H., Zhang, Y., Si, X., Yao, Z., Liang, Z. (2022). MDS2-C3PF: A medical data sharing scheme with cloud-chain cooperation and policy fusion in IoT. Symmetry, 14(12): 2479. https://doi.org/10.3390/sym14122479

[16] Shi, S., He, D., Li, L., Kumar, N., Khan, M.K., Choo, K.K.R. (2020). Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. Computers & Security, 97: 101966. https://doi.org/10.1016/j.cose.2020.101966

[17] El Bekkali, C., Sabiri, K., Ettaloui, N., Sabiri, N., Idrissi, N. (2023). A blockchain-based architecture and framework for cybersecure smart cities. IEEE Access, 11: 76359-76376. https://doi.org/10.1109/ACCESS.2023.3296482

[18] Al-Omrani, E.N., Humayun, M. (2023). Securing electronic health records (EHR) from tampering using blockchain. In Advances in Systems Engineering, pp. 397-410. https://doi.org/10.1007/978-3-031-40579-2_38

[19] Dragonas, E., Lambrinoudakis, C., Kotsis, M. (2023). IoT forensics: Analysis of a HIKVISION's mobile app. Forensic Science International: Digital Investigation, 45(Suppl.): 301560. https://doi.org/10.1016/j.fsidi.2023.301560

[20] Hutchinson, S., Stanković, M., Ho, S., Houshmand, S., Karabiyik, U. (2023). Investigating the privacy and security of the SimpliSafe security system on Android and iOS. Journal of Cybersecurity and Privacy, 3(2): 145-165. https://doi.org/10.3390/jcp3020009

[21] Kamaruzaman, K.N., Hussein, Z., Fikry, A. (2023). Factors affecting behavioural intention to use mobile health applications among obese people in Malaysia. E+M Ekonomie a Management, 26(1): 45-64. https://doi.org/10.15240/tul/001/2023-1-003

[22] Tawalbeh, L.A., Muheidat, F., Tawalbeh, M., Quwaider, M. (2020). IoT privacy and security: Challenges and solutions. Applied Sciences, 10(12): 4102. https://doi.org/10.3390/app10124102

[23] Agbo, C.C., Mahmoud, Q.H., Eklund, J.M. (2019). Blockchain technology in healthcare: A systematic review. Healthcare, 7(2): 56. https://doi.org/10.3390/healthcare7020056

[24] Zhuang, Y., Sheets, L.R., Chen, Y.W., Shae, Z.Y., et al. (2020). A patient-centric health information exchange framework using blockchain technology. IEEE Journal of Biomedical and Health Informatics, 24(8): 2169-2176. https://doi.org/10.1109/JBHI.2020.2993072

[25] Velmovitsky, P.E., de Souza, P.A.D.S.E., Vaillancourt, H., Donovska, T., et al. (2020). A blockchain-based consent platform for active assisted living: Modeling study and conceptual framework. Journal of Medical Internet Research, 22(8): e20832. https://doi.org/10.2196/20832

[26] Ghosh, P.K., Chakraborty, A., Hasan, M., Rashid, K., Siddique, A.H. (2023). Blockchain application in healthcare systems: A review. Systems, 11(1): 38. https://doi.org/10.3390/systems11010038

[27] Nguyen, D.C., Pathirana, P.N., Ding, M., Seneviratne, A. (2019). Blockchain for secure EHRs sharing of mobile cloud based e-health systems. IEEE Access, 7: 66792-66806. https://doi.org/10.1109/ACCESS.2019.2917555

[28] Wang, Z., Wang, L., Xiao, F.A., Chen, Q., Lu, L., Hong, J. (2021). A traditional Chinese medicine traceability system based on lightweight blockchain. Journal of Medical Internet Research, 23(6): e25946. https://doi.org/10.2196/25946

[29] Ndri, A. (2023). The applications of blockchain to cybersecurity. https://repository.stcloudstate.edu/msia_etds/141/.

[30] Rupanetti, D., Kaabouch, N. (2024). Combining edge computing-assisted internet of things security with artificial intelligence: Applications, challenges, and opportunities. Applied Sciences, 14(16): 7104. https://doi.org/10.3390/app14167104

[31] Sahu, S.K., Mazumdar, K. (2024). Exploring security threats and solutions techniques for internet of things (IoT): From vulnerabilities to vigilance. Frontiers in Artificial Intelligence, 7: 1397480. https://doi.org/10.3389/frai.2024.1397480

[32] Alshammari, B.M. (2023). AIBPSF-IoMT: Artificial intelligence and blockchain-based predictive security framework for IoMT technologies. Electronics, 12(23): 4806. https://doi.org/10.3390/electronics12234806

[33] Martínez, J., Durán, J.M. (2021). Software supply chain attacks, a threat to global cybersecurity: SolarWinds' case study. International Journal of Safety and Security Engineering, 11(5): 537-545. https://doi.org/10.18280/ijsse.110505

[34] Selvarajan, S., Srivastava, G., Khadidos, A.O., Khadidos, A.O., et al. (2023). An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems. Journal of Cloud Computing, 12(1): 38. https://doi.org/10.1186/s13677-023-00412-y

[35] Dorri, A., Kanhere, S.S., Jurdak, R., Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. In 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, pp. 618-623

https://doi.org/10.1109/PERCOMW.2017.7917634

[36] Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet of Things Journal, 5(2): 1184-1195. https://doi.org/10.1109/JIOT.2018.2812239

[37] Fernández-Caramés, T.M., Fraga-Lamas, P. (2018). A review on the use of blockchain for the Internet of Things. IEEE Access, 6: 32979-33001. https://doi.org/10.1109/ACCESS.2018.2842685

[38] Dutta, P., Choi, T.M., Somani, S., Butala, R. (2020). Blockchain technology in supply chain operations: Applications, challenges and research opportunities. Transportation Research Part E: Logistics and Transportation Review, 142: 102067. https://doi.org/10.1016/j.tre.2020.102067

[39] Tian, F. (2016). An agri-food supply chain traceability system for China based on RFID and blockchain technology. In 2016 13th International Conference on Service Systems and Service Management (ICSSSM), Kunming, China, pp. 1-6. https://doi.org/10.1109/ICSSSM.2016.7538424

[40] Khan, M.A., Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82: 395-411. https://doi.org/10.1016/j.future.2017.11.022

[41] Khrais, L.T. (2020). IoT and blockchain in the development of smart cities. International Journal of Advanced Computer Science and Applications (IJACSA), 11(2). https://doi.org/10.14569/IJACSA.2020.0110220

[42] Atlam, H.F., Wills, G.B. (2019). Technical aspects of blockchain and IoT. Advances in Computers, 115: 1-39. https://doi.org/10.1016/bs.adcom.2018.10.006

[43] Azaria, A., Ekblaw, A., Vieira, T., Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. In 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, pp. 25-30. https://doi.org/10.1109/OBD.2016.11

[44] Balhareth, G., Alsolami, T., Ilyas, M. (2023). IoT big data privacy using blockchain technology: A survey. In Proceedings of the 14th International Multi-Conference on Complexity, Informatics and Cybernetics (IMCIC 2023), pp. 58-63. https://doi.org/10.54808/IMCIC2023.01.58

[45] Ahad, A., Tahir, M., Sheikh, M., et al. (2023). A comprehensive review on 5G-based smart healthcare network security: Taxonomy, issues, solutions and future research directions. Array, 18: 100290. https://doi.org/10.1016/j.array.2023.100290

[46] Ferrag, M.A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., Janicke, H. (2020). Blockchain technologies for the Internet of Things: Research issues and challenges. IEEE Internet of Things Journal, 6(2): 2188-2204. https://doi.org/10.1109/JIOT.2018.2882794

[47] Fromhart, S., Therattil, L. (2016). Making blockchain real for customer loyalty rewards programs. Deloitte Center for Financial Services. https://www.finextra.com/finextra-downloads/newsdocs/us-fsi-making-blockchain-real-for-loyalty-rewards-programs.pdf.

[48] Jafar, U., Aziz, M.J.A., Shukur, Z. (2021). Blockchain for electronic voting system—Review and open research challenges. Sensors, 21(17): 5874. https://doi.org/10.3390/s21175874

[49] Atlam, H.F., Alenezi, A., Alassafi, M.O., Wills, G.B. (2018). Blockchain with Internet of Things: Benefits, challenges, and future directions. International Journal of Intelligent Systems and Applications, 10(6): 40-48. http://doi.org/10.5815/ijisa.2018.06.05

[50] Wang, T., Wu, Q., Chen, J., Chen, F., et al. (2024). Health data security sharing method based on hybrid blockchain. Future Generation Computer Systems, 153: 251-261. https://doi.org/10.1016/j.future.2023.11.032

[51] Saleh, A.M.S. (2024). Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review. Blockchain: Research and Applications, 5(3): 100193. https://doi.org/10.1016/j.bcra.2024.100193

[52] Matnee, Y.A., Albawi, S. (2024). A systematic mapping study on security threats and solutions in social media environments. International Journal of Safety & Security Engineering, 14(6): 1817-1824. https://doi.org/10.18280/ijsse.140616

[53] Sinha, R. (2024). The role and impact of new technologies on healthcare systems. Discover Health Systems, 3(1): 96. https://doi.org/10.1007/s44250-024-00163-w

[54] Owaid, M.A., Hammoodi, A.S. (2024). Evaluating machine learning and deep learning models for enhanced DDoS attack detection. Mathematical Modelling of Engineering Problems, 11(2): 493-499. https://doi.org/10.18280/mmep.110221