e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 5, May 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

SSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 5, May 2024 |

| DOI:10.15680/IJMRSET.2024.0705163 |

Deep Learning-Based Threat Detection with Blockchain-Enabled IoT Security

Rakesh Jain, Dr.Sathish Ramchandra Tormal

Scholar, Department of Computer Science and Engineering, Sunrise University, Alwar, Rajasthan, India

Research Supervisor, Professor, Department of Computer Science and Engineering, Sunrise University, Alwar, Rajasthan, India

ABSTRACT: The rapid growth of the Internet of Things (IoT) has transformed modern digital infrastructure by enabling billions of interconnected devices to communicate and exchange data across diverse environments such as smart homes, healthcare systems, industrial automation, and smart cities. However, the increasing number of IoT devices also introduces significant security challenges due to limited device resources, heterogeneous architectures, and the absence of centralized security management. Traditional security mechanisms often fail to effectively detect and prevent sophisticated cyber threats such as distributed denial-of-service (DDoS) attacks, malware injection, spoofing, and unauthorized access within IoT networks. To address these challenges, this study proposes a hybrid security framework that integrates deep learning-based threat detection with blockchain technology to enhance the security, transparency, and reliability of IoT communication systems. The proposed framework utilizes deep learning algorithms to analyze large volumes of network traffic and device behavior data in order to accurately identify malicious patterns and anomalies in real time. Advanced deep learning models, such as convolutional neural networks (CNN) and recurrent neural networks (RNN), are employed to automatically learn complex features from IoT data streams, enabling efficient detection of both known and unknown cyber threats. These models improve the accuracy and speed of intrusion detection compared to traditional rule-based or machine learning approaches. In addition to intelligent threat detection, blockchain technology is incorporated to provide a decentralized, tamper-resistant, and transparent security infrastructure for IoT networks. Blockchain ensures secure data storage, distributed trust management, and immutable logging of security events without relying on a centralized authority.
.

KEYWORDS: Internet of Things (IoT), Deep Learning, Blockchain Technology, Cybersecurity.

I. INTRODUCTION

The rapid growth of the Internet of Things (IoT) has transformed the way devices communicate, interact, and exchange information across digital networks. IoT refers to a vast ecosystem of interconnected devices such as sensors, smart home appliances, wearable devices, industrial machines, healthcare monitoring systems, and autonomous vehicles that collect and share data through the internet. These devices are designed to improve efficiency, automation, and decision-making across various domains including healthcare, smart cities, agriculture, transportation, and industrial automation. However, the increasing number of connected devices has also introduced significant security challenges. Many IoT devices are resource-constrained and lack robust security mechanisms, making them highly vulnerable to cyberattacks such as data breaches, unauthorized access, distributed denial-of-service (DDoS) attacks, malware injection, and device hijacking. As IoT networks continue to expand, ensuring secure communication, reliable data exchange, and effective threat detection has become a critical research area.

Traditional security solutions often struggle to protect IoT networks effectively due to their centralized architecture, scalability limitations, and inability to handle the dynamic and heterogeneous nature of IoT environments. Centralized security systems create single points of failure where attackers can compromise the entire network by targeting a central server or authority. Additionally, IoT devices generate enormous volumes of data continuously, making it difficult for conventional security monitoring tools to analyze patterns and detect threats in real time. These limitations highlight the need for advanced security frameworks that combine intelligent threat detection with decentralized data protection mechanisms. In this context, emerging technologies such as deep learning and blockchain have gained significant attention as promising solutions for strengthening IoT security.

SSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 5, May 2024 |

| DOI:10.15680/IJMRSET.2024.0705163 |

Deep learning, a subset of machine learning, has demonstrated remarkable capabilities in analyzing complex data patterns and detecting anomalies in large datasets. Unlike traditional rule-based security systems, deep learning models can automatically learn features from network traffic, device behavior, and communication patterns without requiring extensive manual feature engineering. Techniques such as convolutional neural networks (CNN), recurrent neural networks (RNN), and long short-term memory (LSTM) networks are particularly effective in identifying malicious activities within IoT environments. By analyzing network traffic and behavioral data, deep learning models can detect previously unknown attacks, recognize suspicious patterns, and classify threats with high accuracy. These capabilities make deep learning an ideal approach for developing intelligent intrusion detection systems that can operate in dynamic IoT networks where new vulnerabilities and attack strategies constantly emerge.

Despite the advantages of deep learning-based threat detection, data integrity and trust management remain major concerns in IoT environments. IoT devices often communicate over insecure networks, and attackers may attempt to manipulate or tamper with transmitted data. This is where blockchain technology plays a crucial role. Blockchain is a decentralized and distributed ledger technology that records transactions in a secure, transparent, and immutable manner. Each transaction is stored in a block and linked to the previous block using cryptographic techniques, forming a chain of records that cannot be altered without consensus from the network participants. This decentralized structure eliminates the need for a central authority and significantly reduces the risk of data tampering, unauthorized access, and single points of failure.

Integrating blockchain technology with IoT networks provides several important security benefits. First, blockchain enables secure device authentication by maintaining a decentralized registry of authorized devices. This ensures that only trusted devices can join the network and participate in communication. Second, blockchain enhances data integrity by storing transaction records in an immutable ledger, making it extremely difficult for attackers to modify or falsify information. Third, blockchain-based smart contracts can automate security policies and access control mechanisms within IoT networks. Smart contracts are self-executing programs that enforce predefined rules and conditions for device interactions, ensuring that communication occurs only under authorized circumstances. These capabilities contribute to a more secure and trustworthy IoT ecosystem.

II. RESEARCH OBJECTIVES

One of the central objectives of this research is to develop an intelligent deep learning-based threat detection model capable of identifying malicious activities within IoT networks. IoT systems generate massive amounts of data from multiple sensors and devices, making them vulnerable to various forms of cyberattacks. Deep learning algorithms such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), and Autoencoders have demonstrated strong capabilities in identifying patterns and anomalies within large datasets. The research will focus on leveraging these deep learning models to analyze IoT traffic data, detect abnormal behavior, and classify different types of attacks with high accuracy. The objective is to design a model that can automatically learn from network traffic patterns and adapt to evolving threats without requiring constant manual updates. By training the deep learning model on labeled and real-world IoT datasets, the study seeks to achieve improved detection rates and reduced false positives, thereby strengthening the security of IoT communication systems.

Another important objective of this research is to integrate blockchain technology into the IoT security framework to ensure data integrity, transparency, and decentralized trust management. Traditional centralized security systems often rely on a single authority to manage authentication and data storage, which creates vulnerabilities such as single points of failure and potential data tampering. Blockchain technology provides a decentralized ledger that securely records transactions in a tamper-resistant manner, making it an ideal solution for protecting sensitive IoT data. The research aims to design a blockchain-enabled architecture where IoT devices, gateways, and network nodes participate in a distributed ledger system that records security events and device interactions. By using cryptographic techniques and consensus mechanisms, blockchain can ensure that the recorded data cannot be altered or manipulated by malicious actors. The objective is to create a secure and transparent communication environment where all IoT transactions are verified and recorded in a trustworthy manner.

The research also aims to develop a secure communication protocol for IoT networks that leverages blockchain and deep learning technologies to protect data transmission between devices. IoT devices often communicate over wireless networks, which makes them susceptible to interception, spoofing, and replay attacks. This research seeks to design a communication mechanism that incorporates encryption, authentication, and blockchain-based verification processes to ensure that only legitimate devices can participate in the network. Smart contracts may be utilized to automate security policies, device authentication, and access control procedures. The objective is to establish a secure communication

SSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 5, May 2024 |

| DOI:10.15680/IJMRSET.2024.0705163 |

framework that not only protects the confidentiality and integrity of data but also provides efficient authentication mechanisms that are suitable for resource-limited IoT devices.

Another key objective of this research is to implement a decentralized trust management system that uses blockchain technology to evaluate and maintain the trustworthiness of IoT devices within the network. In large-scale IoT environments, it is difficult to determine whether a device is behaving legitimately or maliciously. The proposed framework will use blockchain to store device reputation scores, behavioral logs, and transaction histories in a secure and immutable manner. Deep learning models can analyze these records to identify suspicious patterns and update trust scores accordingly. By combining blockchain-based transparency with intelligent threat analysis, the research aims to establish a reliable trust management mechanism that helps prevent compromised devices from affecting the overall network security. This objective is essential for maintaining a stable and resilient IoT ecosystem where devices can interact safely without relying on centralized authorities.

III. METHODOLOGY

The proposed study develops a deep learning-based threat detection system integrated with blockchain technology to enhance security in Internet of Things (IoT) networks. The methodology is designed to ensure secure communication, reliable data integrity, and effective detection of malicious activities within IoT environments. The framework combines the pattern recognition capabilities of deep learning models with the decentralized and tamper-resistant characteristics of blockchain technology. The methodology consists of several stages including system architecture design, data collection and preprocessing, model development using deep learning, blockchain integration, threat detection, and performance evaluation.

The first stage of the methodology focuses on designing the overall architecture of the proposed system. The architecture is composed of four main components: IoT devices, edge computing layer, deep learning-based threat detection module, and a blockchain network. IoT devices such as sensors, smart appliances, and wearable devices generate large volumes of network traffic and application data. These devices communicate with the edge layer where initial data processing and monitoring take place. The edge layer acts as an intermediate platform that collects traffic data and forwards relevant information to the deep learning module for analysis. The blockchain network is responsible for securely storing security logs, alerts, and transaction records. This decentralized structure ensures that security events cannot be altered or tampered with, thereby improving trust and transparency in the system.

The second stage involves data collection and dataset preparation for training and testing the deep learning model. Network traffic data is collected from IoT devices using monitoring tools and network sniffing techniques. Publicly available IoT security datasets such as network intrusion datasets or IoT botnet datasets can also be utilized to simulate different attack scenarios. The collected data typically includes parameters such as source and destination IP addresses, packet size, communication protocols, port numbers, timestamps, and device identifiers. After collection, the raw data undergoes preprocessing to remove noise and irrelevant information. Data preprocessing includes steps such as data cleaning, normalization, feature extraction, and labeling. Feature selection techniques are applied to identify the most relevant attributes that contribute to detecting security threats. This step is essential for improving the efficiency and accuracy of the deep learning model.

The next stage of the methodology focuses on developing the deep learning-based threat detection model. In this framework, deep learning techniques such as Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks, or hybrid CNN-LSTM models can be used for identifying malicious activities in IoT network traffic. These models are capable of learning complex patterns and temporal relationships within large datasets. The preprocessed dataset is divided into training, validation, and testing sets. During the training phase, the deep learning model learns the patterns associated with normal behavior and different types of cyber attacks such as Distributed Denial of Service (DDoS), malware injection, spoofing, and unauthorized access attempts. The training process involves optimizing model parameters using algorithms such as stochastic gradient descent or Adam optimizer. The validation dataset is used to fine-tune the model and prevent overfitting, while the testing dataset evaluates the final performance of the model.

Once the deep learning model is trained, the system proceeds to the real-time threat detection stage. In this stage, network traffic from IoT devices is continuously monitored and analyzed by the trained deep learning model. The model processes incoming data and classifies network behavior as either normal or malicious. If the system detects suspicious activity or an attack pattern, an alert is generated immediately. This automated detection mechanism allows

SSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 5, May 2024 |

| DOI:10.15680/IJMRSET.2024.0705163 |

the system to respond quickly to potential threats and minimize damage to the network. The detection results, along with associated metadata such as timestamps and device IDs, are then forwarded to the blockchain network for secure storage and verification.

IV. BACKGROUND

The rapid expansion of the Internet of Things (IoT) has significantly transformed modern technological ecosystems by enabling seamless connectivity among billions of devices such as sensors, smart appliances, industrial machines, healthcare devices, and vehicles. IoT networks facilitate real-time data collection, monitoring, and automated decision-making across various domains including smart cities, healthcare, agriculture, transportation, and industrial automation. However, while IoT offers tremendous benefits in terms of efficiency, automation, and data-driven insights, it also introduces serious security challenges. IoT devices are often resource-constrained in terms of computational power, memory, and energy, which makes the implementation of traditional security mechanisms difficult. Moreover, many IoT devices are deployed in open and distributed environments where they are highly vulnerable to cyber threats such as malware attacks, data manipulation, denial-of-service attacks, spoofing, and unauthorized access. As a result, ensuring secure communication and reliable data transmission within IoT networks has become one of the most critical concerns in modern cybersecurity research.

One of the key challenges in IoT security arises from the centralized architecture used in many conventional network management systems. Traditional security frameworks often rely on centralized servers for authentication, data storage, and access control. This centralization creates a single point of failure, making the system vulnerable to targeted cyberattacks. If a centralized server is compromised, the entire IoT network may be affected, leading to data breaches, system disruption, or unauthorized control of devices. Additionally, the heterogeneity of IoT devices, the massive volume of data generated, and the dynamic nature of network connections further complicate the implementation of effective security solutions.

Blockchain technology has emerged as a promising solution to address several of these security challenges. Blockchain is a distributed and decentralized ledger technology that allows multiple participants to securely record, verify, and share transactions without relying on a central authority. Each transaction recorded in the blockchain is cryptographically secured and linked to previous blocks, creating an immutable chain of records that cannot easily be altered or tampered with. The decentralized nature of blockchain enhances transparency, trust, and accountability within a network, making it suitable for securing IoT systems. By integrating blockchain into IoT architectures, devices can securely exchange data, authenticate identities, and maintain a trustworthy record of communication events. Furthermore, blockchain can support smart contracts, which are self-executing programs that automatically enforce predefined security policies and access control rules.Despite the advantages of blockchain in providing decentralized security, blockchain alone may not be sufficient to detect sophisticated cyber threats in IoT networks. Modern cyberattacks are becoming increasingly complex, adaptive, and difficult to identify using traditional rule-based security systems. Attackers frequently exploit vulnerabilities in network protocols, device firmware, and communication channels, making it challenging to detect malicious behavior in real time. In this context, artificial intelligence (AI), particularly deep learning techniques, has gained significant attention as a powerful tool for cybersecurity. Deep learning is a subset of machine learning that utilizes multi-layered neural networks to automatically learn patterns and representations from large datasets. Unlike traditional algorithms that rely on manually designed features, deep learning models can analyze complex data structures and identify hidden patterns associated with malicious activities.

Deep learning-based threat detection systems have shown promising results in identifying network anomalies, intrusion attempts, and malware attacks in IoT environments. Techniques such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), long short-term memory (LSTM) networks, and autoencoders are widely used to analyze network traffic patterns and detect abnormal behavior. These models can process large volumes of IoT data and continuously improve their detection accuracy through training on historical attack datasets. For instance, LSTM models are particularly effective in analyzing sequential network traffic data, enabling the detection of time-based attack patterns such as distributed denial-of-service (DDoS) attacks. Similarly, autoencoder-based anomaly detection models can identify deviations from normal network behavior, which may indicate potential cyber threats. Integrating deep learning with blockchain technology creates a hybrid security framework that combines the strengths of both approaches. Blockchain provides a decentralized and tamper-resistant infrastructure for secure data storage and communication, while deep learning offers intelligent threat detection capabilities. In such a hybrid framework, IoT devices can record communication events and network transactions on a blockchain ledger, ensuring transparency and data integrity. At the same time, deep learning models can analyze the recorded data to identify suspicious activities or potential security breaches. Once a threat is detected, the blockchain network can automatically trigger predefined

SSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 5, May 2024 |

| DOI:10.15680/IJMRSET.2024.0705163 |

security responses through smart contracts, such as isolating compromised devices, blocking malicious traffic, or alerting network administrators.

Another important advantage of integrating deep learning with blockchain is the enhancement of trust management within IoT networks. In large-scale IoT deployments, devices often interact with unknown or newly connected nodes, making it difficult to establish trust. Blockchain can maintain a secure record of device identities and past interactions, enabling a decentralized trust management system. Deep learning algorithms can further analyze behavioral patterns of devices to determine trust levels and detect malicious nodes attempting to infiltrate the network. This combination significantly improves the reliability and resilience of IoT systems against internal and external threats. However, implementing a deep learning and blockchain-enabled IoT security framework also presents several challenges. One major concern is the computational overhead associated with deep learning algorithms and blockchain operations. Many IoT devices have limited processing power and cannot directly execute complex neural network models or participate in blockchain consensus mechanisms. To address this issue, researchers are exploring edge computing and fog computing architectures where computationally intensive tasks are performed at edge nodes or gateways instead of individual IoT devices. Edge servers can run deep learning models to analyze network traffic and communicate with the blockchain network to record security events.

V. LITERATURE REVIEW

The rapid growth of the Internet of Things (IoT) has transformed modern digital infrastructure by enabling billions of interconnected devices to communicate and exchange data across heterogeneous networks. IoT systems are widely used in smart cities, healthcare, industrial automation, transportation, and environmental monitoring. However, the increasing number of connected devices has significantly expanded the attack surface, making IoT environments highly vulnerable to cyber threats such as distributed denial of service (DDoS), malware attacks, spoofing, and data manipulation. Traditional security mechanisms designed for centralized networks often fail to provide adequate protection for IoT environments due to the limited computational capabilities of IoT devices and the dynamic nature of network traffic. As a result, researchers have explored advanced approaches that combine deep learning techniques with decentralized technologies such as blockchain to improve threat detection and secure communication in IoT networks.

Deep learning has emerged as a powerful tool for cybersecurity due to its ability to automatically extract complex features from large datasets and detect anomalies in network traffic. Conventional intrusion detection systems (IDS) based on rule-based or classical machine learning algorithms often struggle to identify unknown attacks and evolving threat patterns. Deep learning models such as convolutional neural networks (CNN), recurrent neural networks (RNN), long short-term memory (LSTM), and deep belief networks have demonstrated strong capabilities in detecting sophisticated cyber attacks in IoT environments. These models analyze network traffic patterns, device behavior, and communication anomalies to identify malicious activities with high accuracy. Studies have shown that deep learning-based intrusion detection systems can significantly outperform traditional machine learning methods in terms of detection rate, adaptability, and scalability. For instance, research on deep learning approaches for IoT threat detection reports that advanced neural network models can detect complex attack patterns such as DDoS, botnet activity, and malware propagation more effectively than conventional systems.

Despite the effectiveness of deep learning models, IoT security systems still face major challenges related to data integrity, trust management, and centralized data processing. Most deep learning-based intrusion detection systems rely on centralized architectures where large volumes of network data are collected and processed in a central server. This approach introduces several risks, including data tampering, single points of failure, and privacy concerns. Blockchain technology has therefore been proposed as a complementary solution to address these limitations. Blockchain is a decentralized distributed ledger that records transactions in a secure and immutable manner using cryptographic mechanisms and consensus protocols. By eliminating the need for a central authority, blockchain ensures transparency, trust, and integrity of data exchanged among IoT devices. The decentralized nature of blockchain also enhances system resilience against cyber attacks and unauthorized modifications.

Researchers have increasingly focused on integrating blockchain technology with artificial intelligence to create more robust IoT security frameworks. In such hybrid systems, blockchain acts as a trusted platform for storing and sharing network information, while deep learning algorithms analyze the stored data to detect malicious activities. The combination of these technologies enables real-time monitoring and secure decision-making in IoT environments. Blockchain ensures that the data used by AI models cannot be manipulated by attackers, thereby improving the reliability of threat detection mechanisms. Furthermore, blockchain can verify device identities and enforce access

SSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 5, May 2024 |

| DOI:10.15680/IJMRSET.2024.0705163 |

control policies, allowing only authenticated devices to participate in the network. This integration allows AI-based intrusion detection systems to operate in a decentralized environment where security events are verified through distributed consensus.

Several studies have proposed blockchain-enabled deep learning frameworks for intrusion detection and threat intelligence in IoT systems. For example, a blockchain-based cyber-security threat intelligence framework utilizes deep neural networks to analyze network traffic and predict potential security threats. In this architecture, blockchain is used to store security logs and share threat intelligence among distributed nodes, while deep learning models perform intrusion alert prediction based on extracted features from network data.

VI. DISCUSSION

The rapid expansion of the Internet of Things (IoT) has significantly transformed modern digital infrastructure by enabling billions of interconnected devices to communicate and exchange data across various applications such as smart homes, healthcare, industrial automation, transportation, and smart cities. However, this widespread adoption has also introduced serious security challenges due to the resource-constrained nature of IoT devices, heterogeneous network architectures, and the massive volume of data generated by these systems. Traditional security mechanisms often fail to provide adequate protection because they rely on centralized architectures that can become single points of failure and are not capable of handling sophisticated and evolving cyber threats. As a result, integrating advanced technologies such as deep learning and blockchain has emerged as a promising solution for enhancing threat detection and ensuring secure communication within IoT environments.

Deep learning plays a crucial role in improving threat detection capabilities in IoT networks. Unlike traditional machine learning methods, deep learning models can automatically extract complex patterns and hidden features from large datasets without requiring extensive manual feature engineering. This capability makes them highly suitable for analyzing the massive and continuously generated data streams in IoT systems. Techniques such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), and long short-term memory networks (LSTMs) have been widely applied for detecting anomalies, malware, botnet activities, and distributed denial-of-service (DDoS) attacks in IoT networks. These models learn from historical network traffic data and identify abnormal behaviors that may indicate potential security threats. For instance, deep learning algorithms can analyze packet flows, communication patterns, and device behavior to detect unusual activities in real time, thereby enabling proactive security responses before attacks cause significant damage.

Despite the effectiveness of deep learning in identifying threats, IoT networks still face major challenges related to data integrity, trust management, and secure data sharing. This is where blockchain technology provides an additional layer of security. Blockchain is a decentralized and distributed ledger technology that allows secure and transparent storage of data across multiple nodes without the need for a central authority. Each transaction recorded on the blockchain is cryptographically secured and linked to the previous block, making it extremely difficult for attackers to alter or manipulate stored information. In the context of IoT security, blockchain can be used to ensure the integrity of device data, authenticate communication between devices, and maintain a tamper-proof record of network activities.

VII. CONCLUSION

The integration of deep learning with blockchain technology offers a promising and comprehensive solution for enhancing threat detection and security in Internet of Things (IoT) networks. As IoT devices continue to grow rapidly across industries such as healthcare, smart cities, transportation, and industrial automation, the need for robust and intelligent security mechanisms becomes increasingly critical. Traditional security approaches often struggle to cope with the scale, heterogeneity, and resource constraints of IoT environments. These limitations expose IoT systems to various cyber threats including malware attacks, distributed denial-of-service (DDoS) attacks, data tampering, unauthorized access, and privacy breaches. In this context, the combination of deep learning techniques for intelligent threat detection and blockchain technology for decentralized trust management creates a powerful hybrid security framework capable of addressing many of the vulnerabilities present in modern IoT infrastructures. Deep learning plays a vital role in identifying complex and evolving cyber threats within IoT networks. Unlike traditional rule-based intrusion detection systems, deep learning models such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), long short-term memory (LSTM) networks, and autoencoders can analyze large volumes of network traffic data and learn hidden patterns associated with malicious behavior. These models continuously improve their detection capabilities through training on diverse datasets, allowing them to recognize both known and previously unseen threats. This ability is particularly important in IoT environments where new attack patterns frequently emerge.

SSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 5, May 2024 |

| DOI:10.15680/IJMRSET.2024.0705163 |

By leveraging deep learning algorithms, IoT security systems can achieve higher detection accuracy, faster response times, and improved adaptability to changing attack strategies. Moreover, deep learning models can automate threat analysis, reducing the reliance on manual monitoring and enabling real-time anomaly detection across distributed IoT devices.

However, while deep learning provides intelligent detection capabilities, it still relies on centralized data management systems in many traditional architectures. Centralized systems are vulnerable to single points of failure, data manipulation, and unauthorized access. This is where blockchain technology significantly strengthens the overall security framework. Blockchain introduces a decentralized and immutable ledger that records transactions and communications among IoT devices in a transparent and tamper-resistant manner. Each block in the chain contains cryptographically secured data that cannot be altered once verified by the network. This ensures data integrity and accountability across all participating nodes. In a blockchain-enabled IoT environment, devices can securely exchange information without relying on a central authority, thereby reducing the risk of system compromise.

The integration of blockchain with deep learning-based threat detection further enhances trust and reliability within IoT ecosystems. Blockchain can securely store logs of detected threats, device identities, and access permissions, ensuring that security events are permanently recorded and cannot be manipulated by malicious entities. Smart contracts, which are programmable scripts stored on the blockchain, can automate security policies such as authentication, access control, and response mechanisms when suspicious activity is detected. For example, if a deep learning model identifies abnormal traffic behavior from a particular IoT device, a smart contract can automatically isolate that device from the network, preventing further damage. This automated response capability strengthens the resilience of IoT systems against coordinated cyberattacks.

REFERENCES

1. Rathore, S., Pan, Y., & Park, J. H. (2019). BlockDeepNet: A Blockchain-Based Secure Deep Learning for IoT Network. Sustainability, 11(14), 3974.
2. Latif, S., Ilyas, M. S. B., Imran, A., Abosaq, H. A., & Alzubaidi, A. (2024). Machine Learning Empowered Security and Privacy Architecture for IoT Networks with Blockchain Integration. Intelligent Automation & Soft Computing, 39(2), 353–379.
3. Sagduyu, Y. E., Shi, Y., & Erpek, T. (2019). IoT Network Security from the Perspective of Adversarial Deep Learning. arXiv Preprint.
4. Rahman, M. S. A. M. H. (2020). A Lightweight Blockchain Framework for Secure Data Analytics in IoT-Based Smart Cities. IEEE Network.
5. Kim, H., Park, J., Bennis, M., & Kim, S. (2020). Blockchained On-Device Federated Learning. IEEE Communications Letters.
6. Frauenthaler, P., Sigwart, M., Spanring, C., et al. (2020). ETH Relay: A Cost-Efficient Relay for Ethereum-Based Blockchains. IEEE International Conference on Blockchain.
7. Wang, Z., Yang, L., Wang, Q., Liu, D., Xu, Z., & Liu, S. (2019). ArtChain: Blockchain-Enabled Platform for Art Marketplace. IEEE International Conference on Blockchain.
8. Yang, X., Chen, Y., & Chen, X. (2019). Effective Scheme Against 51% Attack on Proof-of-Work Blockchain. IEEE International Conference on Blockchain.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com