A Comprehensive Investigation of Blockchain-Enabled Federated Learning Approaches for DDoS Attack Mitigation in Internet of Things Environments

Jiaxuan Wu

Computer Science College, Wenzhou Kean University, Wenzhou, China

1305983@wku.edu.cn

**Abstract.** With the rapid spread of Internet of Things (IoTs), various electronic technology products form a regional network, which dramatically enhances digital interconnectivity. But it also introduced significant security risks, notably DDoS attacks. These attacks exploit the vulnerabilities of resource-constrained IoT devices to form botnets that overwhelm network services, as seen in the Mirai incident. This study aims to analyze these security challenges and propose decentralized, blockchain-based mitigation strategies. This paper focuses on integrating blockchain with FED-IDS and deep learning to improve DDoS detection and prevention. By storing immutable model updates and access control policies on a distributed ledger, the system enhances transparency, trust, and fault tolerance, reducing risks posed by centralized defenses. Smart contracts are utilized for dynamic access control and blacklisting of malicious traffic, while deep learning algorithms analyze high-dimensional network traffic to detect complex attack patterns. Furthermore, a blockchain-managed federated learning architecture is employed in vehicular networks to prevent data leakage, coordinate model training, and resist poisoning attacks. Experiments using datasets such as ToN\_IoT demonstrate that blockchain-enhanced FED-IDS improves detection accuracy and resilience over traditional IDS approaches. However, limitations including reliance on labeled data, blockchain latency, and scalability bottlenecks are identified. Future work is encouraged to explore semi-supervised learning, lightweight consensus algorithms, and adaptive trust mechanisms. Overall, this research underscores blockchain’s potential in securing IoT environments against sophisticated, distributed DDoS threats while revealing areas for further optimization.

# INTRODUCTION

The rapid spread of Internet of Things (IoT) devices has significantly enhanced technological connectivity but has also introduced substantial security vulnerabilities, notably Distributed Denial of Service (DDoS) attacks. DDoS attack floods the target server with a flood of fake traffic, making it unable to handle requests from legitimate users, resulting in service outages or severe performance degradation. In the IoT environment, attackers use infected devices to form botnets to coordinate large-scale DDoS attacks, further exacerbating the threat. The widespread deployment of IoT devices, inadequate security configurations, and limited processing power make them vulnerable to botnet-driven intrusions that can disrupt critical services and overwhelm networks. Traditional centralized security models often struggle to effectively mitigate these threats due to inherent single points of failure and scalability limitations, highlighting the need for decentralized and resilient security frameworks [1].

Blockchain technology, characterized by its decentralized and immutable ledger system, has emerged as a promising solution for enhancing IoT security against DDoS attacks. By storing data at different network nodes, blockchain avoids as much as possible the entire node being breached due to a single point of failure, enhancing the fault tolerance rate. For instance, Jawahar.et al presents a novel system that leverages machine learning algorithms for real-time DDoS attack detection and employs blockchain technology to store and block malicious IP addresses through software-defined networking. The system enhances security measures beyond traditional DDoS mitigation systems [2].Besides, Aguru.et al focus on building multi-vector DDoS attack defense framework based on blockchain (OTI-IoT). The framework combining blockchain and deep learning technologies, it aims to enhance the defense capability of IoT network against multi-vector DDoS attacks. The system includes two phases: attack prevention stage and attack detection stage. Attack Prevention (IPS Module): when IoT devices request services, the IPS module verifies their identities and access rights through smart contracts [3]. If malicious behavior is detected, immediately block its access request to prevent the occurrence of attacks. Attack Detection (IDS Module): IDS instances deployed on verification nodes use deep learning models to analyze network traffic and identify multi-vector DDoS attacks. Once an attack is detected, an alert message is generated and broadcast to the entire network through a smart contract. Malicious IP addresses in the alert information are added to the blacklist, and the IPS module updates the access control policy accordingly to further enhance protection. It is worth mentioning that when using six verification nodes, the time for detecting multi-vector DDoS attacks is 5 minutes, which is superior to other existing methods. In the attack prevention of both the network layer and the application layer, OTI-IoT shows a relatively high prevention rate [3].

This review aims to: (1) analyze the challenge and security issues in IoT, especially DDoS attack; (2) Evaluate the effectiveness of blockchain-based DDoS mitigation security mechanisms; (3) Look for future research directions to improve blockchain integrated IoT security solutions. This study divides defense strategies into blockchain attack detection and Federated Intrusion Detection System, decentralized authentication, and optimized application of deep learning.

# Preliminaries Of IOT And DDoS Attack

## Challenges and Security Issues in IoT

IoT refers to devices that have sensors, computing functions, and software, allowing them to connect and share data with other devices or systems through the Internet or other networks [4-7]. The IoT encompasses electronics, communication, and computer science engineering. IoT has revolutionized the way devices communicate and interact, enabling seamless connectivity across various domains such as smart homes, healthcare, transportation, and industrial automation. However, this rapid proliferation also brings forth a multitude of challenges.

### Resource Constraints and Weak Security Mechanisms

Most IoT devices are designed with a focus on cost and energy efficiency, resulting in limited computing power, storage space and battery life. These restrictions make it difficult to implement traditional security measures (such as complex encryption algorithms, firewalls and intrusion detection systems) on these devices, thereby reducing overall security.

### Lack of Unified Standards and Security Update Mechanisms

There are numerous types of IoT devices and many manufacturers, and there is a lack of unified security standards and protocols. Different manufacturers use different communication protocols (such as MQTT, CoAP, Zigbee, etc.) and operating systems, lacking a unified authentication and encryption mechanism. For example, some devices use plaintext HTTP to transfer sensitive data instead of encrypted HTTPS. Some devices lack remote update functions and are unable to promptly fix known vulnerabilities, thus being exposed to risks for a long time.

In addition, many IoT devices are equipped with default usernames and passwords (such as admin/admin) when they leave the factory, but users often do not change them. Attackers can easily scan the network through automated scripts and brute-force crack these devices. It led to a terrible accident: Mirai Botnet Attack

According Krebs, B., Bonderud, D et al. reported, the Mirai botnet was first discovered by MalwareMustDie (a white-hat malware research group) in August 2016 and was used in some of the largest and most extensive DDoS attacks, including the attack on the website of computer security journalist Brian Krebs on September 20, 2016. The attack on the French network host OVH, and the DDoS attack on Dyn. in October 2016 [8, 9].

It led to many Internets service paralysis including Twitter, Netflix, GitHub, Reddit, Airbnb, Spotify, PayPal, CNN et al dozens of internationally renowned websites were blocked or completely disrupted. The peak attack traffic reached as high as 1.2 Tbps, setting a historical record for the highest DDoS attack at that time

### Large-scale Deployment and Poor Physical Security

IoT devices are typically deployed on a large scale in various environments, including homes, enterprises, and public places. These devices are often unattended, have poor physical security and are vulnerable to being taken control by attackers. Once compromised, attackers can use these devices to form huge botnets and launch large-scale DDoS attacks. The characteristics of IoT devices, such as resource constraints, the lack of unified security standards, large-scale deployment, and poor physical security, make them ideal targets for DDoS attacks.

## Evaluation and Optimization of the DDoS Mitigation Security Mechanism

### Federated Intrusion Detection System

Traditional Intrusion Detection Systems (IDS) are usually deployed in local networks and are difficult to adapt to large-scale attack detection in a distributed environment, especially when facing DDoS attack sources distributed in multiple geographical locations. Federated learning (FL) a machine learning technique. In this case, multiple entities collaboratively train a model while keeping the data dispersed [10], rather than stored in central. A defining characteristic of FL is data heterogeneity. Because client data is decentralized, data samples held by each client may not be independently and identically distributed.

Federated Intrusion Detection System (FIDS) avoids the leakage of original traffic data and allows multiple edge nodes to collaboratively train the detection model without sharing the original data [11].

But FL essentially relies on the upload of local models, while the central server cannot view the original data. If a certain client is attacked or deliberately injected with abnormal training data, the model parameters trained by it will contaminate the final global model. What’s worse, hiding training data might allow attackers to inject backdoors into the global model [12]. Attackers can exploit backdoor attacks, for example, making the model perform normally in most cases but output false judgments as long as specific features (such as specific IP patterns) are input [13]. Besides, FIDS also has the disadvantage of data forgery and untrustworthy nodes. It’s a great choice to cite blockchain technique.

### Blockchain-Enabled Intrusion Detection Systems

Blockchain is a decentralized ledger system, featuring distributed storage, data immutability, consensus verification, and transparent traceability [14]. Each round of model parameter upload is recorded on the chain in the form of transactions to ensure model traceability, non-forgery and responsibility traceability, which can trace back those abnormal nodes that are invaded by DDoS attacks. Furthermore, smart contracts can automatically execute model verification and abnormal node penalty mechanisms. Distributed consensus avoids single-point bottlenecks, enhances system robustness, and reduces the risk of central nodes being attacked by DDoS.

### Blockchain and Deep Learning-based Federated Intrusion Detection System in Smart Transportation Systems

Deep learning is a branch of machine learning that uses multi-layer neural networks to handle tasks such as classification, regression, and feature representation. These deep neural networks, which have several layers between the input and output, are designed to simulate how the human brain processes information and can be trained similarly to other machine learning models. Each node can train deep models such as CNN, LSTM, and GRU based on local network traffic which are great at identifying covert DDoS attack behaviors from nonlinear and high-dimensional traffic characteristics.

According to Mohamed A et al.’s research, they proposed an innovative Edge Intelligence Blockchain (EIB) framework that integrates blockchain technology with the Vehicular Edge Computing paradigm to enhance data exchange in vehicular networks. This framework facilitates the development of a secure, efficient, and decentralized FED-IDS. Within this system, a consortium blockchain is employed to ensure secure and distributed orchestration of federated training processes for intrusion detection. The local gradient data submitted by participating vehicles is verified for authenticity, while a network of trusted consensus nodes replaces the central server in managing all local model updates. As a result, this approach effectively mitigates the security and privacy vulnerabilities commonly found in traditional federated learning systems [15].

After completing the local FED-IDS training at the industrial edge node, the model parameters need to be uploaded to the central cloud server beyond the authorized blockchain system. The blockchain structure mainly includes the Blockchain Manager (BM), scheduler and validator. First, the contributor's data is sent as a transaction to the nearby BM. The BM is responsible for distributing the blocks to be verified to multiple validators and initiating the consensus process. Eventually, the verified blocks are added to the chain. BM is equivalent to a coordinator, while the validator is similar to a "miner", jointly completing block verification and on-chain recording.

### Evaluation of the Detection Performance of FED-IDS

The research assesses the detection capabilities of the FED-IDS system under two scenarios: traffic originating from external vehicular networks and traffic within in-vehicle networks. Experimental comparisons shown in Table 1 using the ToN\_IoT dataset reveal that traditional FL produces the lowest accuracy at 91.87%. In contrast, the proposed FED-IDS demonstrates notable performance gains, with an accuracy improvement of 2.69% and an F1-score increase of 0.84%. Additionally, by leveraging blockchain’s capacity to filter out malicious or low-quality model updates, the IDS achieves greater efficiency and reliability than conventional cloud-based approaches.

**TABLE 1.** Comparison Between the Detection Performance of the FED-IDS Against the Competing Approaches on the ToN\_IoT Dataset only.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Model | A (%) | P (%) | R (%) | F1-score |
| DeepFed | 92.16 | 92.16 | 92.41 | 92.28 |
| FL | 91.87 | 90.87 | 92.31 | 91.58 |
| FDL | 91.97 | 91.08 | 91.85 | 91.46 |
| FL | 92.02 | 91.03 | 90.11 | 90.57 |
| FED-IDS | 94.85 | 93.17 | 93.09 | 93.13 |

FED-IDS with blockchain and deep learning in smart transportation systems represents a promising advance for detecting and mitigating DDoS attacks in vehicular networks. By leveraging blockchain’s decentralized and tamper-proof nature along with deep learning strong pattern recognition capabilities, the proposed architecture supports privacy-preserving, secure, and scalable detection. Nonetheless, while the approach exhibits several strengths, it also presents important limitations and open challenges that merit further exploration.

# Discussion

By incorporating a blockchain layer into the FED-IDS architecture, model updates can be stored immutably and transparently. Blockchain's consensus mechanism ensures that only verified and authorized updates are included in the ledger, which prevents malicious model injection and guarantees traceability and auditability of model contributions [16]. In smart transportation systems, it promotes blockchain security training and coordination among vehicle edge nodes to enhance the efficiency and flexibility of learning from decentralized data sources.

Blockchain-based FED-IDS enables distributed model management and coordination, it determines the reliability of edge nodes by evaluating the quality of the local model before saving its information to the blockchain, which enhances system resilience and availability, especially under DDoS attack scenarios that aim to overwhelm centralized infrastructure [17].

First, the effectiveness of the proposed FED-IDS strongly depends on supervised learning, which in turn requires large volumes of accurately labeled vehicular traffic data. In real-world STS deployments, especially in highly dynamic and heterogeneous environments, the manual labeling of network flow data is not only time-consuming but also impractical. The lack of labeled datasets limits the generalizability of trained models to unseen attack patterns, including low-frequency or novel DDoS variants.30 Moreover, vehicular data often exhibit imbalances, with benign traffic significantly outnumbering attack samples, which may cause the model to exhibit bias and reduce its detection sensitivity for minority classes. These data-related challenges pose a significant bottleneck for the performance and scalability of supervised FED-IDS systems in production environments [17].

Second, blockchain-related limitations also impact the deployment and performance of the system. The consensus mechanisms used in most existing permissioned or consortium blockchains (e.g., PBFT, PoA) can lead to scalability bottlenecks and computational overhead. This becomes particularly problematic when dealing with frequent model updates and high-throughput data flows in vehicular edge networks [17]. In addition, challenges such as chain forking, limited transaction throughput, and increased latency may hinder real-time decision-making in mission-critical STS operations [17]. Thus, optimizing the blockchain layer for lightweight, real-time consensus in resource-constrained edge environments remains a key issue.

Current blockchain systems and their underlying consensus mechanisms continue to face three major practical challenges: divergence, limited efficiency, and high computational overhead. These issues drive the pursuit of new approaches that can better balance and optimize trade-offs among these competing factors.

Semi-supervised and self-supervised learning: Future work should consider integrating semi-supervised or self-supervised learning techniques to reduce dependence on labeled data [17]. This would allow FED-IDS to learn effectively from large volumes of unlabeled or partially labeled vehicular traffic, thereby improving generalization across diverse attack patterns and reducing annotation costs.

Lightweight blockchain consensus and adaptive trust mechanisms: Developing novel consensus protocols tailored for vehicular environments—such as reputation-based, DAG-based, or federated consensus—could reduce computational burden and improve scalability. In addition, incorporating dynamic trust evaluation models that track node behavior and detect anomaly patterns in model updates would strengthen the system’s resilience to insider attacks and model poisoning [16].

# CONCLUSION

This study addressed the critical DDoS vulnerabilities in IoT environments introduced in the beginning by proposing FED-IDS integrated with deep learning. This paper drew on the tamper-proof and decentralized architecture of blockchain, and enhanced the resilience and traceability of the federated learning-based detection model. Experimental results from smart transportation systems confirmed that the proposed FED-IDS improves detection accuracy and mitigates model poisoning risks compared to traditional FL approaches. Future research will not only focus on refining real-time consensus algorithms and enhancing explainability in security decisions, but also explore more generalized and robust frameworks for IoT defense. This includes adapting semi-supervised and self-supervised learning to reduce reliance on labeled data, developing trust-aware decentralized authentication systems, and promoting cross-domain collaboration across different IoT sectors such as healthcare, smart grids, and manufacturing.

# References

1. P. Kumari, A. K. Jain, A. Seth, and Raghav, “Leveraging blockchain and machine learning to counter DDoS attacks over IoT network,” Multimed. Tools Appl. 84(1), 317–341 (2025).
2. A. Jawahar, P. Kaythry, V. C. Kumar, R. Vinu, R. Amrish, K. Bavapriyan, and V. Gopinaath, “DDoS mitigation using blockchain and machine learning techniques,” Multimed. Tools Appl. 83, 60265–60278 (2024).
3. A. Aguru and S. Erukala, “OTI-IoT: A blockchain-based operational threat intelligence framework for multi-vector DDoS attacks,” ACM Trans. Internet Technol. 24(3), 1–31 (2024).
4. K. Rose, S. Eldridge, and L. Chapin, “The Internet of Things: An overview,” Internet Society (ISOC) 80(15), 1–53 (2015).
5. S. Li, L. D. Xu, and S. Zhao, “The Internet of Things: A survey,” Inf. Syst. Front. 17, 243–259 (2015).
6. F. Xia, L. T. Yang, L. Wang, and A. Vinel, “Internet of Things,” Int. J. Commun. Syst. 25(9), 1101 (2012).
7. S. C. Mukhopadhyay and N. K. Suryadevara, “Internet of Things: Challenges and opportunities,” Springer International Publishing (2014).
8. New Jersey Cybersecurity and Communications Integration Cell, “Mirai Botnet,” [Online]. Available: [https://web.archive.org/web/20161212084605/https://www.cyber.nj.gov/threat-profiles/botnet-variants/mirai-botnet](https://web.archive.org/web/20161212084605/https:/www.cyber.nj.gov/threat-profiles/botnet-variants/mirai-botnet) (2016).
9. unixfreaxjp, “MMD-0056-2016 – Linux/Mirai, how an old ELF malcode is recycled,” MalwareMustDie (2016). [Online]. Available: [https://web.archive.org/web/20160905023500/http://blog.malwaremustdie.org/2016/08/mmd-0056-2016-linuxmirai-just.html](https://web.archive.org/web/20160905023500/http:/blog.malwaremustdie.org/2016/08/mmd-0056-2016-linuxmirai-just.html)
10. P. Kairouz, H. B. McMahan, B. Avent, A. Bellet, M. Bennis, A. N. Bhagoji, K. Bonawitz, Z. Charles, G. Cormode, R. Cummings, and R. G. D’Oliveira, “Advances and open problems in federated learning,” Found. Trends Mach. Learn. 14(1–2), 1–210 (2021).
11. L. U. Khan, I. Yaqoob, N. H. Tran, S. M. A. Kazmi, T. N. Dang, and C. S. Hong, “Federated learning for IoT security: State-of-the-art and future challenges,” IEEE Netw. 35(2), 246–253 (2021).
12. E. Bagdasaryan, A. Veit, Y. Hua, D. Estrin, and V. Shmatikov, “How to backdoor federated learning,” in Proc. 23rd Int. Conf. on Artificial Intelligence and Statistics (AISTATS) (2020). [Online]. Available: <https://arxiv.org/abs/1807.00459>
13. E. Bagdasaryan, A. Veit, and Y. Hua, “Backdoor attacks on federated learning,” arXiv preprint arXiv:1807.00459 (2019).
14. S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system” (2008). [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
15. M. Abdel-Basset, N. Moustafa, H. Hawash, I. Razzak, K. M. Sallam, and O. M. Elkomy, “Federated intrusion detection in blockchain-based smart transportation systems,” IEEE Trans. Intell. Transp. Syst. 23(3), 2523–2537 (2022).
16. J. Zhao, Y. Zhang, H. Song, and R. Yu, “A blockchain-based trust mechanism for federated learning in vehicular networks,” IEEE Trans. Ind. Inform. 17(7), 5109–5118 (2021).
17. C. Liu, Z. Zhang, X. Cheng, and H. Song, “Federated intrusion detection in blockchain-based smart transportation systems,” IEEE Trans. Intell. Transp. Syst. 23(11), 20794–20806 (2021).