PRIVACY-PRESERVING FEDERATED LEARNING WITH DYNAMIC AGGREGATION FOR SOPHISTICATED CYBERATTACKS

UPPALA SARVAN KUMAR
PG Scholar
Department of Computer Science and Engineering
JNTUA College of Engineering, Anantapur
uppalasarvan0@gmail.com

G. PRADEEP REDDY
Assistant Professor
Department of Computer Science and Engineering
JNTUA college of Engineering, Anantapur
pradeepreddyg.cse@jntua.ac.in

ABSTRACT

The rapid growth of Internet of Things (IoT) devices has significantly increased the vulnerability of modern networks to sophisticated cyber threats such as botnets, cryptominers, infostealers, ransomware, and zero-day attacks. Traditional centralized malware detection systems face major challenges including privacy leakage, communication overhead, limited scalability, and vulnerability to adversarial manipulation in large-scale IoT environments. Although Federated Learning (FL) enables collaborative learning without sharing raw device data, existing FL-based approaches often rely on static aggregation mechanisms and lack adaptability against evolving cyberattacks.

To address these limitations, this paper proposes CyberForce, a Privacy-Preserving Federated Reinforcement Learning Framework with Dynamic Aggregation for intelligent malware detection and adaptive cyber defense in IoT environments. The proposed framework integrates Federated Learning for secure distributed model training, Reinforcement Learning (RL) for dynamic defense optimization, and robust aggregation algorithms such as FedAvg, Krum, and Trimmed Mean to mitigate poisoning and adversarial attacks. Deep learning models including CNN, LSTM, and BERT are employed to extract static and dynamic malware features from network traffic and system activities. Experimental results demonstrate that the proposed framework achieves high malware detection accuracy, low detection latency, improved scalability, and strong resilience against sophisticated cyber threats, making it a reliable cybersecurity solution for next-generation IoT systems.

Keywords: IoT Security, Malware Detection, Federated Learning, Reinforcement Learning, Dynamic Aggregation, Deep Learning, Privacy Preservation.

1. INTRODUCTION

The rapid advancement of the Internet of Things (IoT) has transformed various sectors, including healthcare, smart cities, industrial automation, transportation, agriculture, and home automation. Billions of interconnected IoT devices continuously collect, process, and exchange data, enabling intelligent decision-making and real-time monitoring. However, the rapid expansion of IoT networks has also introduced significant cybersecurity challenges due to the resource-constrained nature of IoT devices, heterogeneous communication protocols, and large-scale distributed deployments [1]–[4].

Modern IoT ecosystems have become attractive targets for cybercriminals because many devices possess limited computational power, memory, and security mechanisms. Consequently, sophisticated malware such as botnets, ransomware, cryptominers, spyware, infostealers, worms, and zero-day attacks can rapidly compromise vulnerable devices and spread across interconnected networks. Large-scale attacks, including Distributed Denial-of-Service (DDoS) attacks orchestrated through IoT botnets, have demonstrated the severe consequences of inadequate IoT security, resulting in financial losses, service disruptions, and privacy breaches [2], [5], [6].

Traditional malware detection approaches primarily rely on centralized machine learning architectures, where data collected from distributed devices are transferred to a central server for model training and analysis. Although centralized

methods can achieve high detection accuracy, they suffer from several limitations, including excessive communication overhead, privacy leakage, high storage requirements, single points of failure, and poor scalability in large IoT environments. Moreover, transmitting sensitive device data to centralized servers raises serious privacy concerns and increases the risk of data exposure during communication [2], [4], [7].

Federated Learning (FL) has emerged as a promising distributed machine learning paradigm that enables collaborative model training without requiring IoT devices to share their raw data. Instead, each participating device trains a local model using its private data and transmits only model parameters or gradients to a central aggregation server. This significantly enhances data privacy while reducing communication costs and supporting decentralized intelligence. However, conventional FL frameworks commonly employ static aggregation methods such as Federated Averaging (FedAvg), which are vulnerable to model poisoning, Byzantine failures, and adversarial attacks. Furthermore, these approaches often struggle to adapt to continuously evolving malware families and dynamic cyberattack strategies [7]–[10].

Reinforcement Learning (RL) has recently gained considerable attention for adaptive cybersecurity applications because it enables intelligent agents to learn optimal defense strategies through continuous interaction with dynamic environments. Unlike conventional supervised learning methods, RL continuously improves decision-making based on observed rewards, allowing cybersecurity systems to respond effectively to emerging attack patterns, unknown threats, and changing network conditions. Integrating RL with FL provides an opportunity to develop intelligent and adaptive malware detection systems capable of continuously optimizing security policies while preserving user privacy [11], [12].

In addition, recent advances in deep learning have significantly improved malware detection capabilities. Convolutional Neural Networks (CNNs) effectively learn spatial features from malware representations and network traffic, Long Short-Term Memory (LSTM) networks capture temporal dependencies in sequential system behaviors, and Bidirectional Encoder Representations from Transformers (BERT) provide contextual feature extraction from textual logs and system events. Combining these complementary deep learning models enables comprehensive feature learning from both static and dynamic malware characteristics, thereby improving detection performance [13]–[15].

To overcome the limitations of existing approaches, this paper proposes **CyberForce**, a Privacy-Preserving Federated Reinforcement Learning Framework with Dynamic Aggregation for intelligent malware detection in IoT environments. The proposed framework integrates Federated Learning for secure distributed model training, Reinforcement Learning for adaptive cyber-defense optimization, robust aggregation algorithms including **FedAvg**, **Krum**, and **Trimmed Mean** to resist poisoning attacks, and deep learning models such as **CNN**, **LSTM**, and **BERT** for multi-modal malware feature extraction. The framework aims to improve malware detection accuracy, reduce detection latency, enhance scalability, preserve user privacy, and strengthen resilience against sophisticated adversarial attacks in next-generation IoT ecosystems [8]–[16].

The major contributions of this paper are summarized as follows:

- A novel privacy-preserving Federated Reinforcement Learning framework (**CyberForce**) for intelligent malware detection in IoT environments.
- Integration of Reinforcement Learning with Federated Learning to enable adaptive cyber-defense against evolving malware and zero-day attacks.
- Implementation of robust dynamic aggregation mechanisms, including FedAvg, Krum, and Trimmed Mean, to mitigate poisoning and Byzantine attacks.
- Utilization of CNN, LSTM, and BERT models for comprehensive extraction of static and dynamic malware features.
- Extensive experimental evaluation demonstrating

improved detection accuracy, reduced latency, enhanced scalability, and stronger robustness compared with conventional centralized and federated malware detection approaches.

The remainder of this paper is organized as follows. Section 2 reviews the related work on IoT malware detection, Federated Learning, Reinforcement Learning, and privacy-preserving cybersecurity. Section 3 presents the proposed CyberForce framework and system architecture. Section 4 describes the experimental setup and implementation details. Section 5 discusses the experimental results and performance evaluation. Finally, Section 6 concludes the paper and outlines future research directions.

2. LITERATURE REVIEW

The rapid advancement of Internet of Things (IoT) technologies has introduced significant cybersecurity challenges due to the increasing number of interconnected devices and the growing sophistication of cyberattacks. Researchers have proposed various machine learning, deep learning, federated learning, and reinforcement learning techniques to enhance malware detection and intrusion prevention in IoT environments. This section reviews existing literature related to IoT malware detection, privacy-preserving federated learning, dynamic aggregation, and adaptive cyber defense mechanisms.

Traditional malware detection systems mainly rely on centralized machine learning approaches in which data collected from multiple devices are transferred to a central server for model training and analysis. Although these methods provide high detection accuracy, they suffer from several limitations including privacy leakage, communication overhead, and lack of scalability in large-scale IoT environments [1]. Moreover, centralized architectures introduce single points of failure, making them vulnerable to targeted cyberattacks.

To overcome privacy concerns in distributed systems, Federated Learning (FL) has emerged as an effective decentralized learning paradigm. McMahan et al. [2] introduced the Federated Averaging (FedAvg) algorithm, which enables collaborative model training without sharing raw data among devices. In FL, each client device locally trains the model using private datasets and transmits only model parameters to a central aggregation server. This approach significantly improves privacy preservation and reduces communication costs. Konečný et al. [3] further proposed communication-efficient federated learning techniques to improve scalability in distributed environments.

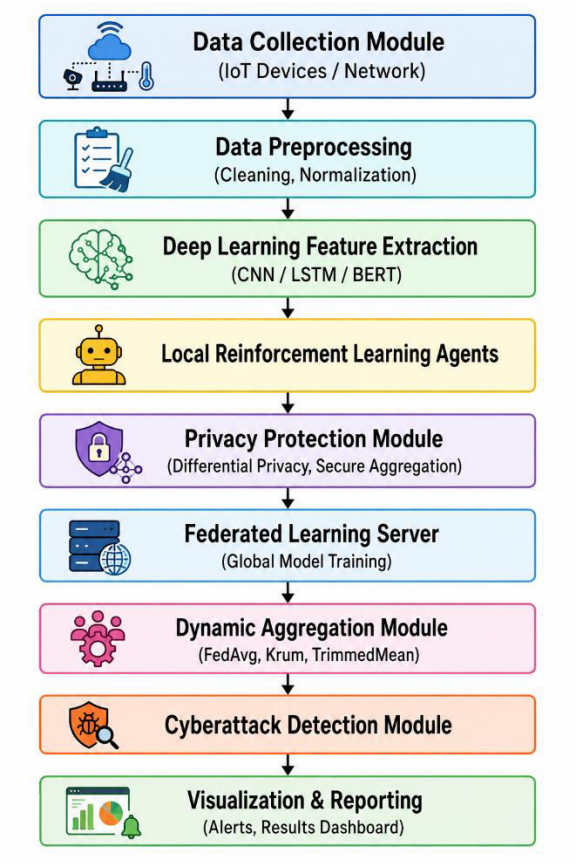
Despite the advantages of federated learning, FL systems remain vulnerable to adversarial and poisoning attacks where malicious clients intentionally manipulate model updates to degrade the global model performance. To address this challenge, Byzantine-resilient aggregation algorithms such as Krum and Trimmed Mean have been proposed. Blanchard et al. [4] introduced the Krum aggregation algorithm to filter malicious updates by selecting gradients that are closest to the majority of honest clients.

Similarly, Yin et al. [5] proposed the Trimmed Mean aggregation mechanism to remove abnormal model updates before aggregation, thereby improving robustness against poisoning attacks.

3. RELATED WORK

Recent advances in IoT have accelerated research on intelligent malware detection using Machine Learning (ML), Deep Learning (DL), Federated Learning (FL), and Reinforcement Learning (RL). Traditional ML algorithms, including Decision Trees, Support Vector Machines, Random Forests, and K-Nearest Neighbors, rely on handcrafted features and show limited performance against zero-day and polymorphic malware [1]–[3]. Deep learning models such as CNN, LSTM, and BERT improve detection accuracy by automatically extracting spatial, temporal, and contextual malware features [4]–[7]. Federated Learning enables privacy-preserving distributed model training without sharing raw data; however, existing approaches primarily depend on static aggregation methods like FedAvg, which remain vulnerable to poisoning and Byzantine attacks [8]–[12]. Robust aggregation techniques such as Krum and Trimmed Mean improve resilience but

lack adaptability [13], [14]. Reinforcement Learning provides adaptive cyber-defense through continuous policy optimization [15], [16]. Nevertheless, integrating FL, RL, dynamic aggregation, and hybrid deep learning for secure IoT malware detection remains largely unexplored, motivating the proposed **CyberForce** framework.



Modules Used in the System – Flow Chart

4. THREAT MODEL

Internet of Things (IoT) environments consist of a large number of heterogeneous devices communicating over distributed networks, making them highly vulnerable to sophisticated cyberattacks. Most IoT devices have limited computational resources, weak authentication mechanisms, and inadequate security configurations, which attackers can exploit to compromise system integrity, confidentiality, and availability. The proposed framework considers several major threats affecting IoT networks.

One significant threat is malware attacks, including cryptominers, infostealers, and botnets. Cryptominers exploit device resources for unauthorized cryptocurrency mining, while infostealers attempt to steal sensitive information such as credentials and personal data. Botnets infect multiple IoT devices and coordinate them to launch large-scale Distributed Denial of Service (DDoS) attacks.

Another critical threat is poisoning attacks in federated learning environments, where malicious clients intentionally send manipulated model updates to corrupt the global model or introduce backdoors. Such attacks reduce detection accuracy and compromise system reliability. Adversaries may also perform evasion attacks by modifying malware behavior to bypass detection systems.

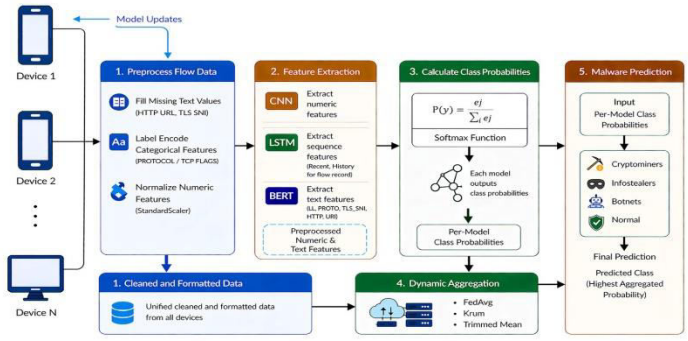


Fig: system architecture

To mitigate these threats, the proposed CyberForce framework employs dynamic aggregation algorithms such as FedAvg, Krum, and Trimmed Mean to filter malicious updates during federated learning. Additionally, reinforcement learning-based strategies dynamically adapt security responses to evolving cyber threats, improving overall system resilience and detection capability.

5. CYBERFORCE FRAMEWORK

The CyberForce Framework is a privacy-preserving and adaptive cybersecurity architecture designed to detect and mitigate sophisticated malware attacks in Internet of Things (IoT) environments. The framework integrates Federated Learning (FL), Reinforcement Learning (RL), dynamic aggregation algorithms, and deep learning models to provide a scalable and intelligent malware detection system while preserving device-level data privacy.

5.1 Local IoT Device Layer

In the proposed framework, heterogeneous IoT devices such as sensors, smart cameras, and embedded systems act as distributed clients. Each device collects local behavioral information including network traffic, system calls, and application activities. Instead of transferring raw data to a centralized server, devices locally train deep learning models using their own datasets. Deep learning architectures such as Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and BERT are utilized to extract both static and dynamic malware features.

5.2 Privacy-Preserving Federated Learning

Federated learning enables collaborative model training without sharing sensitive device data. IoT devices periodically send encrypted model updates to the central aggregation server rather than transmitting raw datasets. This decentralized learning approach improves privacy preservation, reduces communication overhead, and supports scalable deployment across distributed IoT environments.

5.3 Dynamic Aggregation Mechanism

To improve robustness against adversarial attacks, the framework employs dynamic aggregation algorithms including Federated Averaging (FedAvg), Krum, and Trimmed Mean. These aggregation techniques identify and filter malicious or corrupted model updates generated by compromised devices during federated learning, thereby enhancing global model reliability and resilience against poisoning attacks.

5.4 Reinforcement Learning Defense Engine

A Reinforcement Learning (RL) agent dynamically optimizes cybersecurity responses by continuously monitoring system behavior and detected threats. The RL agent selects adaptive defense strategies such as where system configurations are periodically changed to reduce attack surfaces and improve protection against evolving cyber threats.

$$Q(s,a) = Q(s,a) + \alpha[r + \gamma \max Q(s',a') - Q(s,a)]$$

Where:

- $Q(s,a)$ = Q-value for state-action pair
- α = Learning rate
- r = Reward
- γ = Discount factor
- s' = Next state

4.5 Global Aggregation Server

The **Global Aggregation Server** coordinates the federated learning process by collecting model updates from distributed IoT devices. After applying the dynamic aggregation algorithms, the server generates an improved global model and distributes it back to the participating devices. This iterative learning process allows the system to continuously improve malware detection accuracy.

$$w_{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} w_k^t$$

Where:

- w_{t+1} = Global model after aggregation
- w_k^t = Local model from client k
- n_k = Number of samples at client k
- $n = \sum_{k=1}^{K} n_k$ = Total data samples
- K = Number of clients/devices

4.6 Malware Detection Capability

The CyberForce framework is designed to detect multiple malware families commonly targeting IoT systems, including cryptominers, infostealers, and botnets**.** By combining deep learning-based feature extraction with adaptive reinforcement learning policies, the system can identify both known and previously unseen malware behaviors.

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

Where:

- **TP** = True Positives (malware correctly detected)
- **TN** = True Negatives (benign files correctly identified)
- **FP** = False Positives (benign files wrongly detected as malware)
- **FN** = False Negatives (malware missed by the system)

Overall, the CyberForce Framework provides a comprehensive and scalable cybersecurity solution for IoT

environments by integrating privacy-preserving learning, robust model aggregation, and adaptive defense mechanisms. This architecture ensures improved malware detection accuracy, strong resilience against adversarial attacks, and efficient large-scale deployment across distributed IoT networks.

6. EXPERIMENTS

To evaluate the effectiveness of the proposed CyberForce Framework, several experiments were conducted to measure malware detection accuracy, robustness against adversarial attacks, and scalability in Internet of Things (IoT) environments. The experiments validated the integration of Federated Learning (FL), Reinforcement Learning (RL), dynamic aggregation algorithms, and deep learning models.

6.1 Experimental Setup

The experimental environment consisted of multiple simulated IoT devices acting as federated clients. Each device trained a local deep learning model using datasets containing both benign and malicious samples. A central aggregation server coordinated the federated learning process and combined local model updates using FedAvg, Krum, and Trimmed Mean algorithms. The framework was implemented using Python with TensorFlow and PyTorch libraries in a distributed computing environment to simulate large-scale IoT networks.

6.2 Dataset and Malware Categories

The experiments utilized IoT malware datasets containing normal and malicious network traffic. Malware categories included cryptominers, infostealers, and botnets. These datasets provided both static and dynamic behavioral features for effective malware analysis and classification.

6.3 Model Training

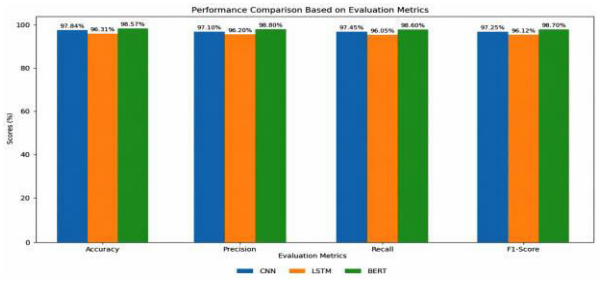
Three deep learning models were employed for feature extraction and malware classification. CNN was used for extracting spatial features from malware binaries and network traffic. LSTM analyzed sequential behavioral patterns of malware activities, while BERT captured contextual relationships in system logs and command sequences. Each IoT device trained models locally and shared only encrypted model parameters with the central server to preserve data privacy.

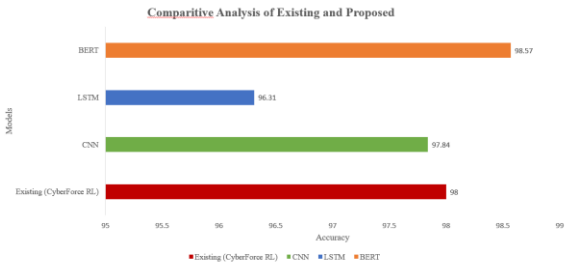
6.4 Evaluation Metrics

The system performance was evaluated using Accuracy, Precision, Recall, F1-Score, and Detection Latency metrics to measure classification performance and response efficiency.

6.5 Experimental Results

Experimental results demonstrated that the CyberForce Framework achieved high malware detection accuracy and strong resilience against adversarial model updates. Dynamic aggregation algorithms significantly improved robustness against poisoning attacks compared to traditional federated learning approaches. Furthermore, reinforcement learning agents dynamically adapted defense strategies, improving threat mitigation and reducing attack impact. The hybrid integration of CNN, LSTM, and BERT enhanced malware feature representation and classification performance. Overall, the framework demonstrated scalability, adaptability, and effective cybersecurity protection for distributed IoT environments.





VI. CONCLUSIONS AND FUTURE WORK

CONCLUSION

In this research, the CyberForce Framework based on Privacy-Preserving Federated Reinforcement Learning was

proposed to address sophisticated cyberattacks in Internet of Things (IoT) environments. The framework integrates Federated Learning, Reinforcement Learning, dynamic aggregation algorithms, and deep learning models to provide a scalable, adaptive, and privacy-preserving malware detection system. CNN, LSTM, and BERT models were utilized for efficient malware feature extraction and classification, enabling the detection of malware families such as botnets, cryptominers, and infostealers. Dynamic aggregation techniques including FedAvg, Krum, and Trimmed Mean improved robustness against poisoning and adversarial attacks, while reinforcement learning agents optimized defense strategies. Experimental results demonstrated high detection accuracy, strong resilience against malicious model updates, and scalability across distributed IoT networks.

FUTURE WORK

Future research can focus on real-time deployment in large-scale IoT environments, blockchain-based secure aggregation, lightweight deep learning models for resource-constrained devices, Explainable AI (XAI) integration, and detection of advanced threats such as ransomware, spyware, and Advanced Persistent Threats (APTs).

REFERENCES

[1] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, “Communication-efficient learning of deep networks from decentralized data,” in *Proc. Int. Conf. Artificial Intelligence and Statistics (AISTATS)*, 2017, pp. 1273–1282.

[2] J. Konečný, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, “Federated learning: Strategies for improving communication efficiency,” *arXiv preprint arXiv:1610.05492*, 2016.

[3] P. Blanchard, R. Guerraoui, and J. Stainer, “Machine learning with adversaries: Byzantine tolerant gradient descent,” in *Advances in Neural Information Processing Systems (NeurIPS)*, 2017.

[4] Y. Yin, S. Chen, K. Ramchandran, and P. Bartlett, “Byzantine-robust distributed learning: Towards optimal statistical rates,” in *Proc. Int. Conf. Machine Learning (ICML)*, 2018.

[5] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge, MA, USA: MIT Press, 2016.

[6] J. Devlin, M. Chang, K. Lee, and K. Toutanova, “BERT: Pre-training of deep bidirectional transformers for language understanding,” in *Proc. NAACL-HLT*, 2019.

[7] R. S. Sutton and A. G. Barto, *Reinforcement Learning: An Introduction*, 2nd ed. Cambridge, MA, USA: MIT Press, 2018.

[8] Q. Yang, Y. Liu, T. Chen, and Y. Tong, “Federated machine learning: Concept and applications,” *ACM Transactions on Intelligent Systems and Technology*, vol. 10, no. 2, pp. 1–19, 2019.

[9] H. Zhang and Y. Wang, “Moving target defense for cyber systems: A survey,” *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 132–154, 2018.

[10] Y. Meidan et al., “N-BaIoT: Network-based detection of IoT botnet attacks using deep autoencoders,” *IEEE Pervasive Computing*, vol. 17, no. 3, pp. 12–22, 2018.