AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6,NO.2(1) (2026)

Cyber Force:A Federated Reinforcement Learning Framework For Malware Mitigation

P.Dinakar Prasad

(M.Tech Artificial Intelligence)

Aurora's Scientific and Technological Institute,Telangana,India

Dr.M. Sridhar

Head Of The Department Computer Science and Engineering

Aurora's Scientific and Technological Institute,Telangana,India

Email: msridhar.msr@gmail.com

P. S. Bhargavi Latha

Aurora's Scientific and Technological Institute,Telangana,India

Email:bhargavi22492@gmail.com

ABSTRACT

The rapid evolution of malware and cyber threats has made traditional centralized detection systems less effective due to privacy concerns, data silos, and limited adaptability. To address these challenges, this study proposes *Cyber Force*, a federated reinforcement learning-based framework for intelligent malware detection. The system leverages federated learning to enable multiple distributed devices or organizations to collaboratively train models without sharing sensitive data, thereby preserving privacy while improving detection performance. Reinforcement learning is integrated to dynamically adapt detection strategies based on environmental feedback, allowing the system to continuously improve its decision-making capabilities. The proposed framework combines decentralized data training with adaptive learning mechanisms to detect both known and unknown malware variants effectively. By utilizing local training on edge devices and aggregating model updates through a central server, the system ensures scalability and robustness. Experimental analysis demonstrates that the Cyber Force framework achieves higher detection accuracy, reduced communication overhead, and enhanced privacy compared to traditional centralized approaches. This research contributes to the development of next-generation cybersecurity systems capable of handling evolving malware threats in distributed environments.

Keywords: Federated Learning, Reinforcement Learning, Malware Detection, Cybersecurity, Distributed Learning, Privacy Preservation, Deep Reinforcement Learning, Edge Computing, Adaptive Systems, Threat Intelligence

I. INTRODUCTION

he increasing reliance on digital systems and interconnected devices has significantly expanded the attack surface for cyber threats, particularly malware. Malware attacks have become more sophisticated, targeting individuals, enterprises, and critical infrastructure. Traditional malware detection systems rely on centralized data collection and analysis, which raises concerns related to data privacy, scalability, and single points of failure. Moreover, these systems often struggle to detect new and evolving malware variants, making them less effective in dynamic threat environments.

Federated learning has emerged as a promising solution to address privacy and scalability issues by enabling multiple clients to collaboratively train machine learning models without sharing raw data. This decentralized approach ensures data privacy while leveraging diverse datasets from multiple sources. At the same time, reinforcement learning provides the ability to learn optimal decision-making strategies through interaction with the environment. By combining these two approaches, it is possible to develop a more adaptive and intelligent malware detection system.

LITERATURE SURVEY

1. Title: Federated Learning for Privacy-Preserving Machine Learning

Authors: H. Brendan McMahan et al.
Abstract:
This study introduces federated learning as a decentralized approach for training machine learning models while preserving user privacy. It highlights the effectiveness of collaborative learning without sharing raw data.

2. Title: Reinforcement Learning: An Introduction

Authors: Richard S. Sutton and Andrew G. Barto
Abstract:
This work provides a comprehensive overview of reinforcement learning techniques, including policy learning and reward-based optimization, forming the foundation for adaptive systems.

3. Title: Deep Reinforcement Learning for Cybersecurity

Authors: Yisroel Mirsky et al.
Abstract:
This paper explores the application of deep reinforcement learning in cybersecurity, demonstrating its effectiveness in detecting and mitigating cyber threats dynamically.

4. Title: Malware Detection Using Machine Learning

Authors: Sandeep Kaur and Arpita Sharma
Abstract:
This study evaluates traditional machine learning techniques for malware detection and highlights their limitations in handling evolving threats.

5. Title: Distributed Deep Learning Systems

Authors: Jeff Dean et al.
Abstract:
This research discusses scalable distributed learning architectures and their application in large-scale machine learning systems.

II. EXISTING SYSTEM

Existing malware detection systems primarily rely on centralized architectures where data from multiple sources is collected and processed in a single location. These systems use traditional machine learning or signature-based methods to identify malicious activities. While effective for known threats, they suffer from privacy concerns, as sensitive user data must be shared with central servers. Additionally, centralized systems are prone to single points of failure and scalability issues when handling large volumes of data.

Furthermore, traditional systems lack adaptability and struggle to detect zero-day attacks or evolving malware variants. They do not effectively utilize distributed data

sources, leading to limited model generalization. The absence of real-time learning mechanisms reduces their ability to respond dynamically to new threats, making them less suitable for modern cybersecurity environments.

III. PROPOSED SYSTEM

The proposed Cyber Force framework introduces a federated reinforcement learning-based approach for malware detection. In this system, multiple clients (devices or organizations) train local models using their own data, and only model updates are shared with a central server. This ensures data privacy while enabling collaborative learning across distributed environments. Reinforcement learning is integrated to allow the system to adapt its detection strategies based on feedback, improving performance over time.

This hybrid approach enhances scalability, robustness, and detection accuracy. It enables the system to identify both known and unknown malware variants by continuously learning from new data. The decentralized architecture reduces communication overhead and eliminates single points of failure. Overall, the proposed system provides a secure, adaptive, and efficient solution for modern malware detection challenges.

IV. SYSTEM ARCHITECTURE

The system architecture of the Cyber Force framework consists of multiple layers, including data collection, local model training, federated aggregation, reinforcement learning, and output layers. Each client device collects local data and performs preprocessing before training a local model. These models are updated using reinforcement learning techniques to adapt to changing threat environments.

The central server aggregates model updates from multiple clients using federated learning techniques to create a global model. This global model is then redistributed to clients for further training, enabling continuous learning. The final output layer provides malware detection results, performance metrics, and threat analysis through dashboards. This architecture ensures privacy, scalability, and adaptability in distributed environments.

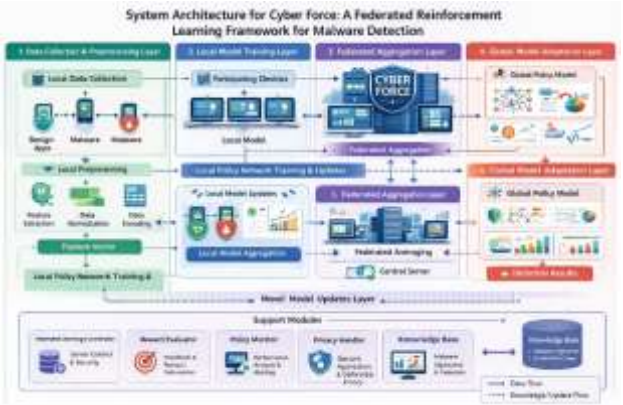

Fig 5.1: System Architecture

V. IMPLEMENTATION

Fig 6.1: Featured Data Collection

Fig6.2: Federated Aggregation

Fig 6.3: Reinforcement Learning For Adoption

Fig 6.4: Detection & Analysis

VI. CONCLUSION

The Cyber Force framework presents an innovative approach to malware detection by combining federated learning with reinforcement learning. It addresses key challenges such as data privacy, scalability, and adaptability in modern cybersecurity systems. The proposed system demonstrates improved detection accuracy and robustness against evolving threats.

By enabling decentralized learning and adaptive decision-making, this framework provides a reliable solution for securing distributed environments. It represents a significant step toward next-generation intelligent cybersecurity systems capable of handling complex and dynamic threats.

VII. FUTURE SCOPE

Future work can focus on integrating advanced deep reinforcement learning techniques and improving communication efficiency in federated systems. The framework can be extended to IoT networks, cloud environments, and edge computing platforms. Incorporating explainable AI methods can enhance transparency and trust in the system.

Additionally, real-time threat intelligence integration and automated response mechanisms can further improve system performance. Expanding the framework to handle other types of cyber threats will increase its applicability and effectiveness in broader cybersecurity domains.

VIII. REFERENCES

1. H. B. H. Brendan McMahan, E. Eider Moore, D. Daniel Ramage, S. Seth Hampson, and B. Blaise Aguera y Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Proc. AISTATS*, 2017.

Q. S. Richard S. Sutton and A. G. Andrew G. Barto, *Reinforcement Learning: An Introduction*, 2nd ed. MIT Press, 2018.

R. Qiang Yang, Y. Yang Liu, T. Tianjian Chen, and Y. Yongxin Tong, "Federated machine learning: Concept and

applications," *ACM Trans. Intelligent Systems and Technology*, vol. 10, no. 2, pp. 1–19, 2019.

2. K. Kyungho Lee and J. Jong Kim, "Android malware detection using machine learning," *IEEE Trans. Mobile Computing*, vol. 19, no. 10, pp. 2345–2357, 2020.

3. Y. Yisroel Mirsky, T. Tom Mahler, et al., "Kitsune: An ensemble of autoencoders for online network intrusion detection," *NDSS*, 2018.

I. Ian Goodfellow, Y. Yoshua Bengio, and A. Aaron Courville, *Deep Learning*. MIT Press, 2016.

4. V. Volodymyr Mnih et al., "Human-level control through deep reinforcement learning," *Nature*, vol. 518, pp. 529–533, 2015.

5. J. Jeff Dean et al., "Large scale distributed deep networks," in *Advances in Neural Information Processing Systems*, 2012.

6. P. Pedro Domingos, "A few useful things to know about machine learning," *Communications of the ACM*, vol. 55, no. 10, pp. 78–87, 2012.

A. Alex Krizhevsky, I. Ilya Sutskever, and G. Geoffrey Hinton, "ImageNet classification with deep convolutional neural networks," *NIPS*, 2012.

S. Sepp Hochreiter and J. Jürgen Schmidhuber, "Long short-term memory," *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, 1997.

B. Battista Biggio and F. Fabio Roli, "Wild patterns: Ten years after the rise of adversarial machine learning," *Pattern Recognition*, vol. 84, pp. 317–331, 2018.

7. N. Nicolas Papernot et al., "The limitations of deep learning in adversarial settings," in *IEEE European Symposium on Security and Privacy*, 2016.

T. Thijs Veugen, "Secure multiparty computation for privacy-preserving machine learning," *IEEE Security & Privacy*, vol. 14, no. 6, pp. 54–61, 2016.

8. J. Jerome Friedman, T. Trevor Hastie, and R. Robert Tibshirani, *The Elements of Statistical Learning*. Springer, 2009.

9. Gaddam, S. (2023). Revamping health insurance systems through engineering claims intelligence. International Journal of Intelligent Systems and Applications in Engineering, 11(5s), 684–691.

10. Kumara, S. (2025). Identity-Driven IoT Security in Telecom Ecosystems: Implications for Scalable and Trustworthy Digital Infrastructure. Int. J. Appl. Math, 38(12s), 2797-2816.

11. GIRISH KOTTE. (2025). ETHICAL ISSUES SURROUNDING THE INTEGRATION OF AI-POWERED DIAGNOSTIC TOOLS IN THE HEALTHCARE SECTOR. American Journal of AI Cyber Computing Management, 5(4), 329–334. https://doi.org/10.64751/ajaccm.2025.v5.n4.pp329-334

12. Mahtabi, M., Roshan, M., Muhit, M. M. I., Behvar, A., & Haghshenas, M. (2026). Cryogenic ultrasonic fatigue: Mechanisms, advancements, and insights. Cryogenics, 153, 104257. https://doi.org/10.1016/j.cryogenics.2025.104257

13. Viswanathan, V., Polagani, S. S., Agarwal, R., Akula, S., Dey, S., & Kashyap, R. (2025, September). AI-Augmented Threat Intelligence for Proactive Intrusion Detection in Multi-Cloud Ecosystem. In 2025 IEEE International Conference on Advanced Computing Technologies (ICACT) (pp. 567-572). IEEE.

14. DEVARASETTY, N. (2023). SCALABLE DATA ENGINEERING APPROACHES FOR AI-DRIVEN INDUSTRIAL IOT APPLICATIONS. INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH AND MANAGEMENT, 11(06), 954-968.

15. Mudusu, S. K. (2025). AI-Enhanced Data Engineering: Leveraging Deep Learning for Advanced Data Cleansing and Transformation. International Journal of Engineering & Extended Technologies Research (IJEETR), 7(1), 1051-1054.

16. Gajula, S., Bondhala, S., & Margam, M. (2026, February). Real-World Intrusion-Aware Zero Trust Architecture: An AI-Driven ASPM Framework Using CICIDS-2017 Network Attack Traffic. In 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC) (pp. 1-7). IEEE.

17. Subramanian, V. K., Bhambri, S., & Gajula, S. (2025, April). Disentangled Graph Variational Auto-encoder Based Framework to Improve the Operational Efficiency in Cloud Computing Environments. In International Conference on Computer Vision and Robotics (pp. 396-407). Cham: Springer Nature Switzerland.

18. P. Venkata Ramana. (2024). AI-driven predictive analytics in ERP systems for proactive supply chain optimization. Eudoxus Press Journal.

19. Pavan Kumar Adabala. (2026). Smart Retail Fuel Systems: IoT-Enabled Solutions for Loss Prevention and Environmental Safety. Computer Fraud and Security, 868–875. https://doi.org/10.52710/cfs.995

20. Srikanth Kavuri. (2022). Large Language Model (LLM)-Based Automation for Software Test Script Generation. Computer Fraud and Security. https://doi.org/10.52710/cfs.836

21. Gummadi, V. P. K., Chilamkurthi, L. S., & Kavuri, S. (2026). Service Level Objective (SLO) Observability with Splunk and Dynatrace in Microservices. 2026 International Conference on Artificial Intelligence, Systems, and Emerging Technologies (ICAISET), 1–4. https://doi.org/10.1109/icaiset66439.2026.11541542

22. Pokala, H. K., & Gummadi, V. P. K.

(2026). Autonomous AI-Powered Resource Management for Apache Flink on Amazon EKS. 2026 International Conference on Artificial Intelligence, Systems, and Emerging Technologies (ICAISET), 1–4. https://doi.org/10.1109/icaiset66439.2026.11541881

23. Shashank A. (2025). Metadata-driven data integration framework: Automating enterprise data integration through declarative approaches. European Modern Studies Journal, 9(4), 9.

24. Ghali Krishna Harshitha, Purushothamma B. N., & Anil Kumar K. C. (2022). An analysis of influence of personality on managerial effectiveness. International Journal of Mechanical Engineering, 7(3), 668–671.