CYBERFORCE++:AN INTELLIGENT MACHINE LEARNING ENABLED FEDERATED REINFORCEMENT LEARNING FRAMEWORK FOR MALWARE MITIGATION WITH REAL-TIME MONITORING AND ALERT MANAGEMENTS IN IOT NETWORKS

[1]Sindhu Priyanka Chadalavada B.Tech,M.Tech(Ph.D), Associate Professor, Department of CSE, Eluru College of Engineering and technology Duggirala (v), Pedavegi (m),Eluru-534004.
[2] M.Prasanthi, M.Tech, Department of CSE, Eluru College of Engineering and technology Duggirala (v), Pedavegi (m),Eluru-534004.

Abstract: The Internet of Things devices are growing fast and that has made it easier for bad people to attack them with sophisticated malware. These attacks can hurt how the devices work if the network is available and if the data is safe. The old way of keeping things safe does not work well because it is slow and not good at keeping private information secret. So, we made something new called Cyber Force++ to help with this problem. Cyber Force++ is a way to keep things safe on the Internet of Things. It uses Machine Learning and something called Federated Reinforcement Learning to stop malware in time and keep data private. It always looks at what the Internet of Things devices doing, like how much work the computer is doing how much memory it is using and what is happening on the network. Then it uses a kind of Machine Learning called Random Forest to look at all this information and figure out if there might be a malware attack. It can even guess how bad the attack might be. Suggest what to do to stop it. What is different about Cyber Force++ is that it uses something called Federated Learning. This means that the devices can work together to learn how to stop malware without sharing all their information. This keeps the data private. Does not use up too much bandwidth. It also uses something called Reinforcement Learning to pick the way to stop the attack based on how bad it is. The system is always. Getting better and it can even change the network to make it harder for bad people to attack. The system also has a dashboard to look at what is happening in real time a way to manage alerts and a way for administrators to log in and manage everything. When we tested Cyber Force++ it worked well. It could find malware attacks predict what to do to stop them and make the network safer. It is a way to keep the Internet of Things safe, from bad people who want to hurt them.

Keywords: Internet of Things (IoT) , Machine Learning ,Random Forest, Federated Learning, Reinforcement Learning, Malware Mitigation, Moving Target Defense, Cyber security, Real-Time Monitoring, Alert Management, Risk Score Prediction

1. INTRODUCTION

The rapid proliferation of the **Internet of Things (IoT)** has transformed the digital landscape by connecting billions of smart devices across domains such as healthcare, industrial automation, smart cities, transportation, agriculture, and home automation. These interconnected devices continuously exchange large volumes of sensitive information, enabling intelligent decision-making and automation. However, the heterogeneous nature of IoT devices, limited computational resources, and large-scale connectivity have significantly increased the attack surface, making IoT ecosystems highly susceptible to sophisticated cyber threats. Among these threats, malware attacks remain one of the most critical security challenges, causing unauthorized access, data breaches, service disruption, and large-scale botnet formation. Traditional malware detection techniques, including signature-based antivirus systems and rule-based intrusion detection methods, are becoming increasingly ineffective against modern malware variants. Advanced malware employs sophisticated evasion techniques such as polymorphism, metamorphism, code obfuscation, and zero-day exploits, enabling malicious software to bypass conventional security mechanisms. Furthermore, centralized machine learning-based security solutions require massive volumes of sensitive data to be transmitted to cloud servers for model training, introducing privacy concerns, communication overhead, high latency, and single points of failure. These limitations make conventional approaches unsuitable for highly distributed and resource-constrained IoT environments where real-time threat detection is essential. Machine Learning (ML) and Deep Learning (DL) techniques have emerged as powerful solutions for intelligent malware detection due to their capability to automatically extract complex behavioral features and identify previously unseen attacks. Supervised learning algorithms such as Random Forest, Support Vector Machine (SVM), Gradient Boosting, and deep neural networks have demonstrated remarkable success in malware classification. Nevertheless, these approaches rely heavily on centralized data collection, which conflicts with privacy regulations and increases the risk of sensitive information leakage. Consequently, privacy-preserving collaborative learning has become an important research direction in cyber security. **Federated Learning (FL)** has recently gained significant attention as a decentralized learning paradigm that enables multiple IoT devices or edge nodes to collaboratively train a global machine learning model without sharing raw data. Instead of transmitting sensitive datasets, only model parameters or gradients are exchanged with a central aggregation server, thereby preserving user privacy while reducing communication costs. Although FL addresses privacy concerns, conventional federated frameworks are still vulnerable to dynamic cyber threats, non-independent and identically distributed (non-IID) data, poisoning attacks, communication delays, and rapidly evolving malware behaviors that require adaptive learning strategies. To overcome these challenges, **Reinforcement Learning (RL)** provides an intelligent decision-making framework capable of learning optimal security policies through

continuous interaction with the environment. RL agents dynamically adapt their mitigation strategies by maximizing cumulative rewards based on observed network conditions and attack behaviors. By integrating RL with Federated Learning, distributed security agents can collaboratively improve malware detection accuracy while independently learning optimal defense mechanisms in real time. Such a federated reinforcement learning architecture offers enhanced adaptability, scalability, and resilience against continuously evolving cyber attacks. In addition to accurate malware detection, effective cyber security requires continuous monitoring of network activities and rapid incident response. Existing security systems often generate excessive false alarms or fail to provide actionable insights for security administrators. Therefore, **real-time monitoring and intelligent alert management** have become essential components of modern cyber security frameworks. Continuous monitoring enables early identification of suspicious behaviors, while adaptive alert prioritization helps security personnel respond quickly to high-risk threats, reducing response time and minimizing system damage. Motivated by these challenges, this paper proposes CYBERFORCE++: An Intelligent Machine Learning Enabled Federated Reinforcement Learning Framework for Malware Mitigation with Real-Time Monitoring and Alert Management in IoT Networks. The proposed framework combines advanced machine learning-based malware detection, privacy-preserving federated learning, adaptive reinforcement learning-based mitigation, and intelligent real-time monitoring to establish a comprehensive cybersecurity solution for IoT ecosystems. Initially, machine learning models deployed at distributed edge nodes analyze device behavior and network traffic to identify malicious activities. Federated learning enables collaborative model training across multiple IoT devices while preserving data privacy and reducing communication overhead. Subsequently, reinforcement learning agents dynamically determine optimal mitigation actions such as traffic isolation, access control, quarantine, or adaptive response based on continuously changing network conditions and threat intelligence. Furthermore, an integrated real-time monitoring and alert management module continuously tracks system behavior, visualizes security events, prioritizes alerts according to threat severity, and supports proactive incident response. The proposed **CYBERFORCE++** framework aims to improve malware detection accuracy, reduce false positive rates, preserve user privacy, minimize response latency, and enhance the overall resilience of IoT networks against both known and previously unseen malware attacks. By integrating intelligent machine learning, federated collaborative learning, reinforcement learning-based adaptive defense, and real-time security monitoring into a unified architecture, the framework provides a scalable, privacy-aware, and autonomous cyber security solution capable of addressing the evolving threat landscape of next-generation IoT environments. Consequently, CYBERFORCE++ represents a significant advancement toward intelligent, decentralized, and self-adaptive malware mitigation for secure and trustworthy IoT networks.

II. LITERATURE SURVEY

2.1 Intrusion Detection in Wireless Sensor Networks. Authors: Zhang et al.

Researchers came up with a system to find activities in wireless sensor networks. This system used rules to figure out what was going on. It worked well for small networks.. It had some big problems. It could not handle networks and it could not find new kinds of malware attacks. The intrusion detection system in sensor networks could not adapt to new attack patterns in wireless sensor networks. This was an issue, for wireless sensor networks.

2.2 Behavior-Based Malware Detection. Authors: Krugelet al

So the idea behind this is that we watch what the computer is doing to see if it is doing anything. We use something called behavioral analysis techniques to monitor what the computer is doing. This way we can find malware that is doing something. We do not need to know what the malware looks like beforehand. The problem, with this is that it needs a lot of power from the computer to work. This is a limitation of Behavior-Based Malware Detection.

3.3 Anomaly-Based Network Intrusion Detection. Authors: Garcia-Teodoro et al

They used math to find out when the network was not behaving like it normally does. The problem, with this was that it gave a lot of warnings. The Anomaly-Based Network Intrusion Detection system had a limitation. The Anomaly-Based Network Intrusion Detection system gave a lot of alarms for no reason.

3.4 Security, Privacy and Trust in IoT. Authors: Sicari et al.

People who study these things say that it is very important to keep our data safe and make sure that Internet of Things devices talk to each other in a way. Internet of Things devices need to be safe from people. You never know when someone will try to hack into Internet of Things devices with malware. Researchers cannot figure out when malware attacks will happen because it is impossible to know everything.

3.5 Machine Learning Based DDoS Detection. Authors: Doshi et al.

This is when Machine Learning algorithms were first used to find Denial of Service attacks in IoT networks. The idea was to use Machine Learning to stop these attacks. One big problem, with this approach was that it relied on collecting

all the data in one place, which's not very practical. So the limitation of Machine Learning Based DDoS Detection was that it needed data collection.

3.6 The Kitsune Lightweight Intrusion Detection System was made in. Authors: Mirsky et al.

This system uses something called auto encoders to find intrusions. It is good at finding things that happen online and it does not use a lot of resources. The problem, with the Kitsune Lightweight Intrusion Detection System is that it does not tell you what to do when it finds something.

3.7 Deep Learning Intrusion Detection. Authors: Shone et al

Deep Learning is great at spotting cyber threats. Deep Neural Networks make it even better at finding these threats. The thing with Deep Learning is that it needs lots of power. This is a problem for Internet of Things devices because they do not have power to run Deep Learning models. Deep Learning needs a lot of energy to work well. Internet of Things devices is not powerful enough to handle Deep Learning. Cyber threats are bad. Deep Learning helps find them.. Deep Learning uses a lot of power which is hard for Internet of Things devices.

3.8 Federated Learning, for Decentralized Systems. Authors: McMahan et al.

Federated Learning is really helpful because it lets people train models together. The good thing about Federated Learning is that people can do this without having to share their data with each other. One big problem, with Federated Learning is that it does not know how to deal with malware problems. Federated Learning has this limitation because it does not have a way to handle malware.

3.9 Reinforcement Learning for Cyber Defense. Authors: Nguyen et al.

Agents using Reinforcement Learning figured out what defense actions to take against cyber threats. They learned this on their own which is pretty cool. One issue with this way of doing things is that it did not keep our data safe. It just did not do that.The Reinforcement Learning, for Cyber Defense did not preserve our data privacy.

3.10 Federated Learning in IoT Security. Authors: Li et al.

So researchers decided to combine Federated Learning with the security measures for Internet of Things. Federated Learning was used to make Internet of Things security better. The main problem, with this idea was that it did not have a way to adapt when something went wrong. The Federated Learning system lacked defense strategies to make Internet of Things security stronger.

III. EXISTING SYSTEM

The Cyber Force framework is used to stop malware in Internet of Things environments. It uses Federated Learning and Reinforcement learning to help devices work together to find the way to defend themselves. Each device looks at its data and trains a Reinforcement Learning agent to find malware and decide what to do about it. The devices then send their information to a place where a global model is made using Federated Learning. This global model is sent back to all the devices to help them get better at finding and stopping malware. The system also changes the network settings often to make it harder for attackers to get in. This way of doing things helps keep information safe and reduces the amount of communication needed. It also helps protect Internet of Things networks from malware threats.

DISADVANTAGES OF EXISTING SYSTEM

1 The system cannot predict malware attacks before they happen because it does not use Machine Learning algorithms to predict attacks. The Cyber Force framework needs to be able to predict malware attacks.

2. The framework does not give a risk score to show how severe a threat is. This makes it hard to know how bad a threat is. The Cyber Force framework should be able to calculate risk scores.

3. There is no way for administrators to see what is happening in the system in time. This makes it hard to monitor the system. The Cyber Force framework needs a real-time monitoring dashboard.

IV. PROPOSED SYSTEM

The Cyber Force++ system is a cyber security framework that helps keep Internet of Things devices safe from malware. It uses Machine Learning, Federated Learning, Reinforcement Learning and Moving Target Defense to stop malware attacks. Cyber Force++ is always watching what Internet of Things devices are doing, like how CPU they use how much memory they need and how much network traffic they make. It looks at all this information to understand how each device behaves. The Cyber Force++ system uses a Random Forest Machine Learning model to guess when malware attacks might happen figure out how risky they are and suggest what to do to stop them. It finds problems before they cause much trouble. Federated Learning helps Internet of Things devices work together to make security models better without sharing information. This keeps everything and does not use too much bandwidth. Reinforcement Learning picks the way to stop malware attacks based on what it thinks might happen. Global Aggregation combines what each device learns to make the whole system smarter. Moving Target Defense always changes the network setup to make it harder for attackers to get in. The CyberForce++ system also has a dashboard that shows what is happening in time a way to manage alerts and a way for administrators to log in. This

makes it easy to see what is going on and manage security. The way CyberForce++ is designed makes it a smart, scalable and private way to keep Internet of Things devices from malware.

ADVANTAGES

- It can guess when malware attacks will happen before they affect Internet of Things devices.
- It calculates risk scores to determine how severe potential threats are.
- It suggests what to do to stop attacks based on what it has learned.
- Administrators can watch what is happening with devices and security in time.

SYSTEM ARCHITECTURE

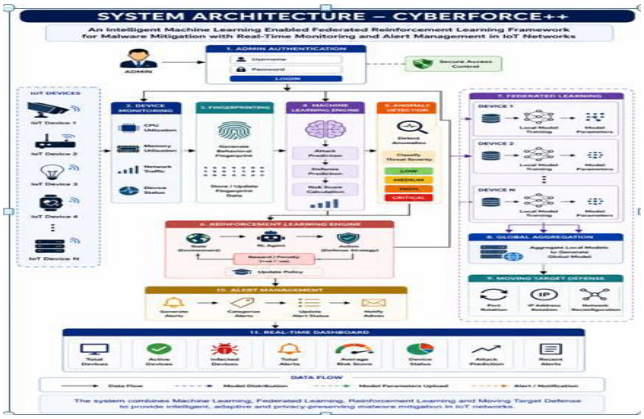

Fig 1: System Architecture

V. UML DIAGRAMS

1. ACTIVITY DIAGRAM

The Cyber Force++ framework has something called an Activity Diagram. This diagram shows what happens in the framework one thing after another. It starts when the administrator logs into the application. Then the system keeps an eye on the IoT devices. Gathers information about how they are working. The system uses this information to make something called fingerprints. These fingerprints are sent to the Machine Learning engine. The Machine Learning engine uses them to predict if there will be an attack to predict how to defend against an attack and to calculate a risk score. The system also looks for things that're not normal which is called Anomaly Detection. If it finds something the Reinforcement Learning engine figures out the best way to defend against it. The CyberForce++ framework also uses something called Federated Learning and Global Aggregation. These two things work together to make the security model better. The framework also uses something called Moving Target Defense. This changes the network configurations a lot so it is harder, for someone to attack it.

Fig 5.1 shows the Activity diagram

2. USECASE DIAGRAM:

The Use Case Diagram shows how the administrator interacts with the CyberForce++ system. The administrator is the person who uses the system. The administrator logs in through authentication. After logging in the administrator can do things. The administrator can watch IoT devices. The administrator can create fingerprints. The administrator can run Machine Learning predictions. The administrator can find anomalies. The administrator can do Reinforcement Learning tasks. The administrator can start Federated Learning. The administrator can do Global Aggregation. The administrator can use Moving Target Defense techniques. The administrator can handle alerts. The administrator can see the real-time dashboard. The Use Case Diagram explains what the administrator can do. It also shows how different parts of the CyberForce++ system work together. The goal is to provide protection against malware, in IoT networks. The administrator and CyberForce++ system work together for this. The CyberForce++ system helps the adm

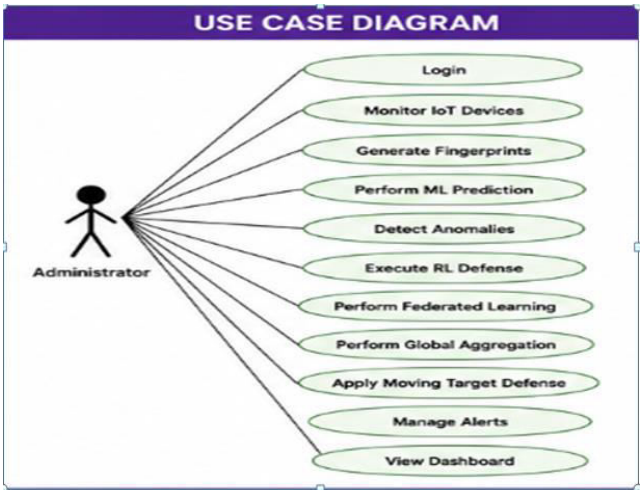

Fig 5.2 Shows the Use case Diagram

3. SEQUENCE DIAGRAM:

The CyberForce++ system uses a thing called a Sequence Diagram to show what happens when different parts of the system talk to each other. This diagram shows how data moves around and how each part of the system communicates with the part to find and stop malware. It all starts when the Administrator logs into the application and gets to the dashboard. The dashboard then asks the Device Monitoring module for information about the devices. This module is always collecting data about how work the devices are doing how much memory they are using and what is happening with the network traffic.

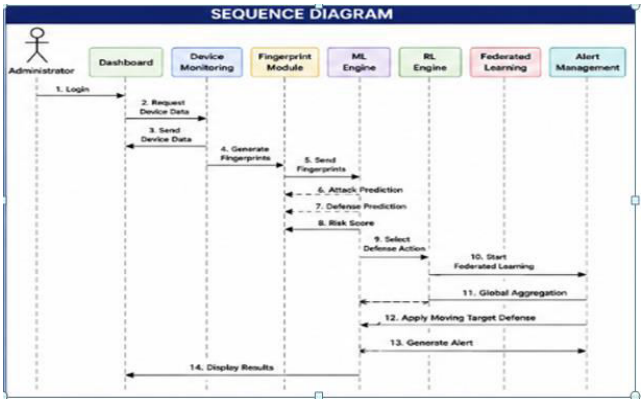

Fig 5.3 Shows the Sequence Diagram

VI. RESULTS

6.1 Output Screens

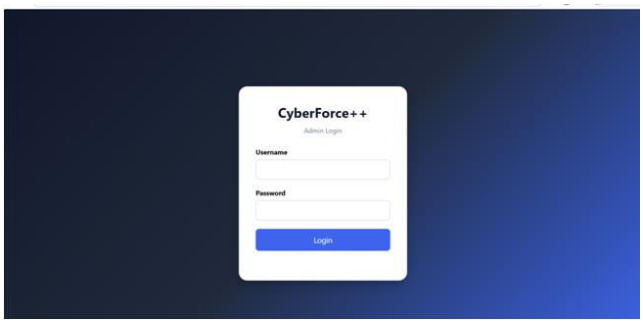

Fig 6.1 Login Page

In above shows the login page

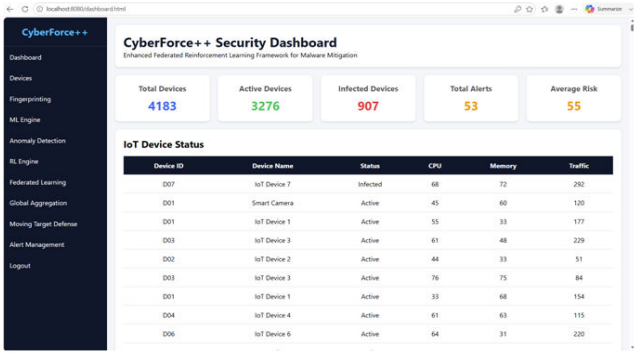

Fig 6.2 Security Dashboard

In above screen shows the security dashboard.

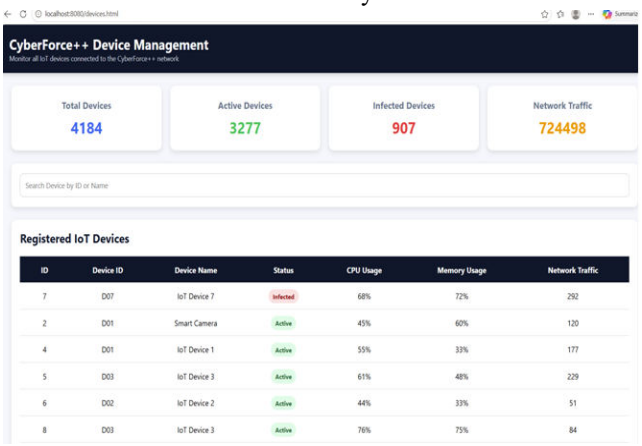

Fig 6.3 Cyber Force++ Device Management

In above screen shows the Cyber Force++ Device Management information

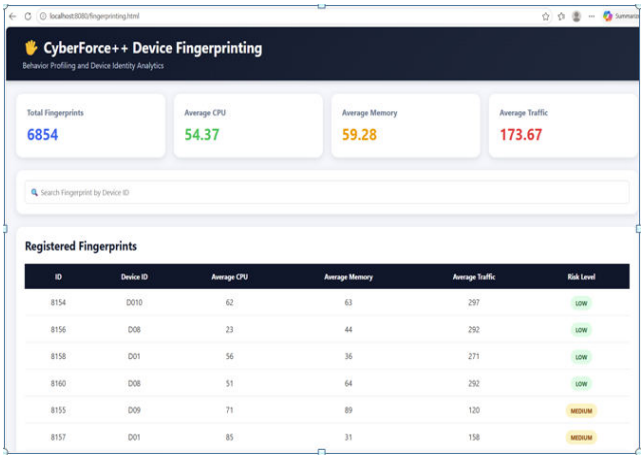

Fig 6.4 CyberForce++ Device Fingerprinting Interface

In above screen shows the CyberForce++ Device Fingerprinting information.

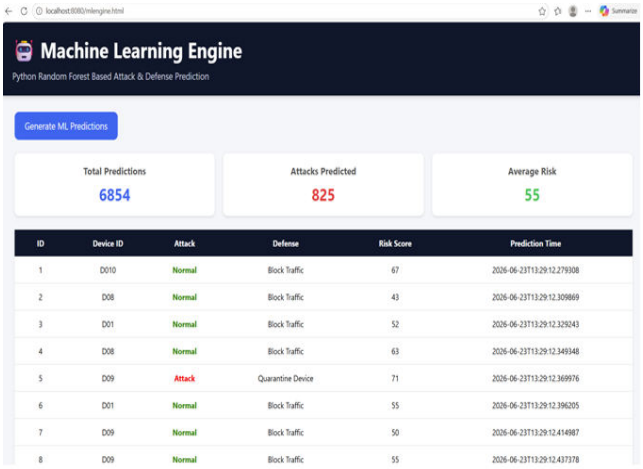

Fig 6.5 Machine Learning Engine Interface

In above screen shows the Machine Learning Engine information.

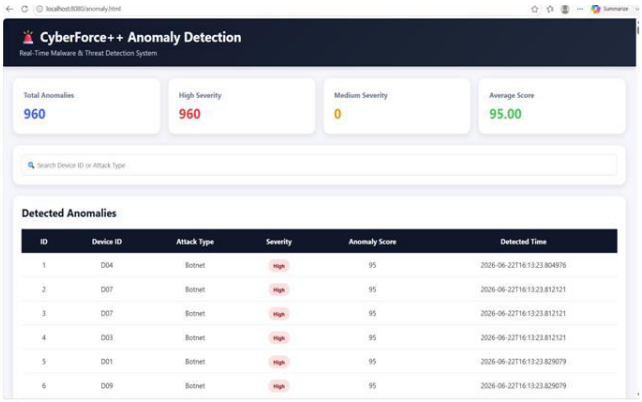

Fig 6.6 Cyber Force++ Anomaly Detection Interface

In the above screen shows the Cyber Force++ Anomaly Detection information.

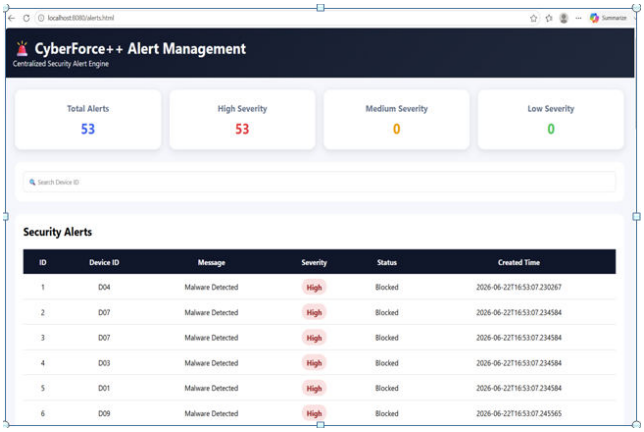

Fig 6.7 Cyber Force++ Alert Management

In above screen shows the Cyber Force++ Alert Management information.

VII. CONCLUSION

The Internet of Things devices are growing fast and that is making cyber security a huge problem. These devices do not have a lot of power to compute things. They are all different from each other. This makes them easy targets for malware attacks. The old ways of keeping them safe are just not good enough because they have a lot of problems like privacy issues and they are too slow to respond to threats. To fix these issues we are suggesting something called CyberForce++. This is a system that uses machine learning and a special kind of learning called reinforcement learning to stop malware from attacking Internet of Things devices. CyberForce++ combines a few techniques like machine learning and federated learning and reinforcement learning to keep malware from getting in. The system is always watching the devices to see what they are doing by checking things like how work the computer is doing and how much memory it is using and what is happening on the network. It uses a kind of computer program to look at all the data and try to predict when a malware attack might happen. The federated learning part helps all the devices work together to learn things without sharing any secret information. Then the reinforcement learning part figures out the way to defend against the malware. CyberForce++ also has some features like a dashboard that shows what is happening in real time and a system that sends out alerts when something is wrong and a way for the people in charge to log in and manage everything. This makes it a lot easier to keep an eye on the network. See if there are any security problems. Cyber Force++ is really good at finding malware. It helps to stop threats before they become a problem in Internet of Things environments. Cyber Force++ is a solution because it is scalable and secure. Cyber Force++ is an improvement over the old systems that were used to stop malware. Cyber Force++ is going to be a part of keeping Internet of Things devices safe, in the future.

VIII. REFERENCES

1. M. Almiani, A. AbuGhazleh and A. Al-Bataineh "CyberForce: A Federated Reinforcement Learning Framework for Malware Mitigation " IEEE Access, vol. 12 Pages 102345–102362 2024.
2. H. Brendan McMahan, E. Moore, D. Ramage, S. Hampson and B. Arcas say in their paper "Communication-Efficient Learning of Deep Networks from Decentralized Data " in Proceedings of the International Conference on Artificial Intelligence and Statistics (AISTATS) on page 1273–1282 in 2017.
3. R. Sutton and A. Barto write about Reinforcement Learning in their book "Reinforcement Learning: An Introduction," 2nd Edition, published by MIT Press, Cambridge, Massachusetts, USA in 2018.
4. L. Breiman writes about Random Forests in Machine Learning Journal, vol. 45 No. 1 Pages 5–32, in 2001.
5. N.. J. Slay present UNSW-NB15 in their paper "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems " in Military Communications and Information Systems Conference (MilCIS) on page 1–6 in 2015.
6. S. Marchal, J. François, R. State and T. Engel discuss Proactive Detection of Advanced Persistent Threats Using Machine Learning in their paper in IEEE Conference on Communications and Network Security on page 1–9 in 2014.

7. S. Jajodia, A. Ghosh, V. Swarup, C. Wang and X. Wang write about Moving Target Defense in their book "Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats " published by Springer Publications in 2011.

8. M. Conti, A. Dehghantanha, K. Franke and S. Watson discuss Internet of Things Security and Forensics in their paper "Internet of Things Security and Forensics: Challenges and Opportunities " in Future Generation Computer Systems vol. 78 Pages 544–546 in 2018.

9. P. Kairouz and others write about Advances and Open Problems in Federated Learning in their paper in Foundations and Trends in Machine Learning vol. 14 No. 1 Pages 1–210, in 2021.

10. Y. LeCun, Y. Bengio and G. Hinton discuss Deep Learning in their paper "Deep Learning," Nature, vol. 521 Pages 436–444 in 2015.

11. Rod Johnson documents Spring Framework in "Spring Framework Reference Documentation " published by Spring Publications in 2024.

12. Craig Walls writes about Spring Boot in his book "Spring Boot in Action " published by Manning Publications in 2016.

13. PostgreSQL Global Development Group documents PostgreSQL in "PostgreSQL Documentation " Version 17 in 2024.

14. F. Pedregosa and others write about Scikit-learn in their paper "Scikit-learn: Machine Learning, in Python " Journal of Machine Learning Research vol. 12 Pages 2825–2830, in 2011.

15. Pandas Development Team Documents Pandas in "Pandas: Python Data Analysis Library " Version 2.2 in 2024.

16. Python Software Foundation Documents Python Language in "Python Language Reference Manual " Version 3.11, in 2024.