IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Malware Botnet Detection Using Deep Reinforcement Learning in IoT Networks

Mrs.k.Rajalakshmi [1], Mrs.Menaka M [2], Mr. Mohamed Sulaimon [3],

[1]Assistant Professor, Department of Electrical and Electronics Engineering, Vel Tech Multi Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Avadi, Chennai, Tamilnadu, India

[2,3] Student, Department of Electrical and Electronics Engineering, Vel Tech Multi Tech Dr.Rangarajan Dr.SakunthalaEngineering College, Avadi, Chennai, Tamilnadu, India

Abstract:

In embedded systems, security is crucial as malware lurks in code, targeting the core with might. Remote execution and privilege escalation intensify the fight. Network breaches exploit vulnerabilities by, intercepting transmissions and casting a shadowy light. Smart grids face threats, including false data injections and disruptions all around. Denial of Service attacks are relentless, overwhelming grid systems and integrity. Smart meters are tampered with, breaching security measures and control. Mitigation strategies include encryption, intrusion detection, and secure boot mechanisms. Regular updates, vulnerability management, and physical security measures are essential. PSO-LSTM, a blend of optimization and accuracy, emerges as a solution for various domains, including rainfall runoff and with Long Short-Term Memory (LSTM) neural networks, has been applied in various ship motion prediction. The Pelican Optimization Algorithm takes flight, balancing exploration and nature-inspired solutions. Minimizing the surface area and focusing on peripherals and hardware security leads to a more secure embedded system landscape.

I INTRODUCTION

Embedded systems are vulnerable to various types of attacks, including malware, software-based, network-based, side-channel, and input crafting attacks. To prevent these, security measures such as regular firmware updates, access limitation, connection monitoring, and integration with security management systems are essential. In the context of smart grids, common cyber-attacks include false data injection, denial of service, smart meter tampering, and hacking smart meters. Defense techniques like encryption, intrusion detection systems, and authentication protocols are being developed to mitigate these threats. Despite these measures, detecting attacks on embedded systems remains a significant challenge, requiring further research and development to address the evolving threat landscape. The Pelican Optimization Algorithm (POA) is a nature-inspired optimization algorithm designed to strike a balance between exploration and exploitation. It simulates the hunting behavior of pelicans and has been applied in various engineering applications. The algorithm involves phases such as moving towards prey (exploration phase) and winging on the water surface (exploitation phase). It has shown competitive performance in providing optimal solutions for optimization problems and has been implemented in MATLAB and educational content on platforms like YouTube. The algorithm has also been enhanced for specific applications, such as cluster head selection in heterogeneous wireless sensor networks. Additionally, the PSO-LSTM model, which combines Particle Swarm Optimization (PSO) fields such as rainfall-runoff simulation, ship motion prediction, moisture content prediction, and water level forecasting, demonstrating improved prediction accuracy and stability.

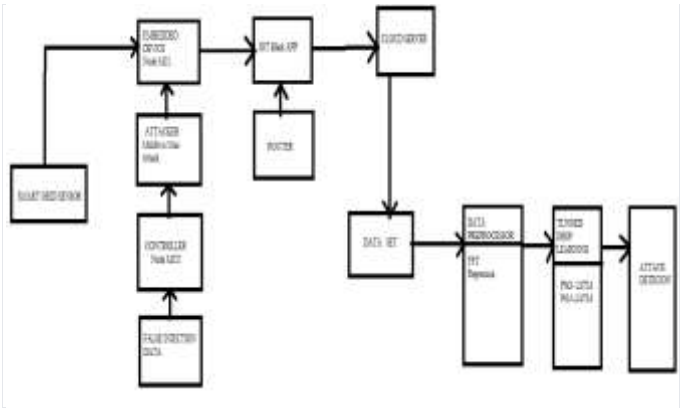


Fig: 1 Block Diagram

II SMART GRID

A smart grid is an advanced electrical grid that utilizes digital technologies, sensors, and software to efficiently match the supply and demand of electricity. It incorporates measures such as advanced metering infrastructure, smart distribution boards, renewable energy resources, and energy-efficient technologies. The smart grid enables two-way communication between suppliers and consumers, leading to more reliable electricity, improved energy efficiency, and increased consumer participation. It also aims to modernize the electric grid to handle the growing demand for power and the integration of new technologies.

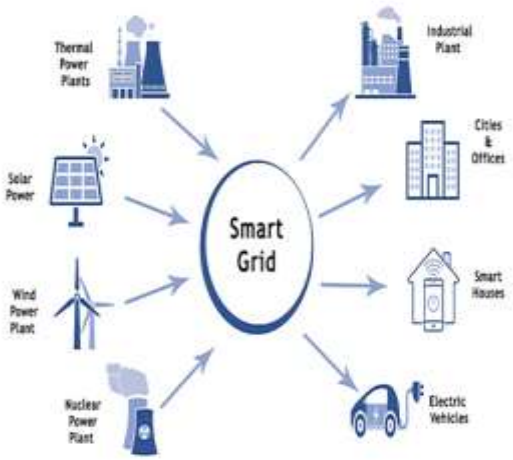


Fig: 2 Smart grid

A. Embedded device

Embedded devices are specialized computer systems designed for specific functions. They consist of a computer processor, memory, and input/output peripheral devices. These devices are found in everyday items such as dishwashers, microwaves, ATMs, routers, and smart phones. They run dedicated software to perform a particular task and are characterized by their small size, low power consumption, and limited capabilities. Examples of embedded systems include central heating systems, GPS systems, fitness trackers, and medical devices. It is important for embedded developers to work with scalable product lines to support the development of product lines with varying levels of functionality.

Fig 3: Embedded device

B IOT Blink app

IoT Blink is a user-friendly mobile app for controlling and managing connected devices. It offers a drag-and-drop interface, allowing users to connect various smart home and industrial products, such as ESP32, Arduino, and Raspberry Pi, to the cloud. The app enables users to create automations, manage access, and integrate with voice assistants like Amazon Echo and Google Home.

Fig 4: IOT Blink app

III CLOUD SERVER

Blynk IoT is a no-code app builder for prototyping, deploying, and managing connected electronic devices at any scale. It is available on the App Store and offers a simple and powerful interface for users to implement their ideas.

Fig 5: Cloud server

A. MIMA

A man-in-the-middle (MITM) attack is a cyber attack where an attacker secretly relays and possibly alters the communications between two parties, leading them to believe they are directly communicating with each other. The attacker positions themselves between the user and the system, potentially intercepting and modifying the data transmitted. MITM attacks can lead to data theft, identity theft, and other security breaches.

Fig 6: Man-in-the-middle attack

B. Controller

Node MCU is an open-source firmware and prototyping board that provides access to GPIO (General Purpose Input/ Output) and is commonly used for IOT projects and remote control applications. It is based on the ESP8266 microcontroller and is known for its ease of use and compatibility with various sensors and actuators. The Node MCU board can be connected to and controlled by other devices, such as gaming controllers, and can also be used to create web-based user interfaces for remote control.

Fig 7: Node MCU Controller

IV FALSE INJECTION DATA

A false data injection attack (FDIA) involves the deliberate alteration or addition of false data into a system, which can lead to misleading information and compromised operations. This type of attack can affect various systems, including smart grids, where adversaries may manipulate sensor readings to mislead control centers. FDIA can lead to significant security threats and the compromise of critical infrastructure, making it essential to develop effective detection and prevention methods.

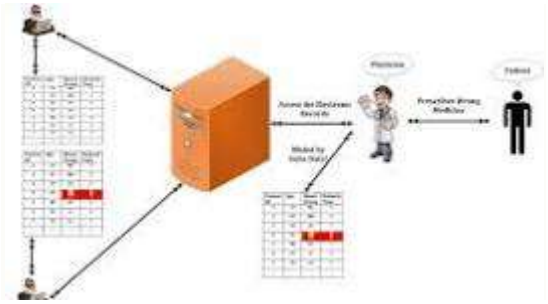


Fig 8: False injection data

A. Router

A router is a networking device that forwards packets between computer networks. It is a crucial component for directing data packets on the Internet. Routers are available in various models and price points to suit different needs and can be purchased from a wide range of retailers.

Fig 9: Router

V DATA SET

A dataset is a collection of data organized in a tabular format, where each column represents a specific variable and each row corresponds to a given member of the dataset. Datasets can be used to analyze various phenomena or to study random numbers. They can be accessed individually or in combination and can be managed as a whole entity. Datasets can be found in various forms, such as lists of integers, tables, or collections of documents or files. In the context of

open data, a dataset is the unit used to measure the information released in a public open data repository. Datasets are essential for machine learning and data analysis applications.

VI DATA PROCESSOR

A.FFT

The Fast Fourier Transform (FFT) is an algorithm that computes the discrete Fourier transform (DFT) of a sequence or its inverse. It is widely used in digital signal processing and converts a signal from its original domain to the frequency domain. The FFT is an optimized method for implementing the DFT and is essential for analyzing frequency components in signals. It is used in various fields, including audio and acoustics measurement, fault analysis, quality control, and condition monitoring of machines or systems.

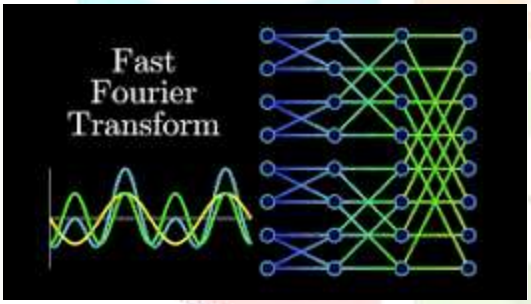


Fig 10: Fast Fourier Transform

B.Regression

Regression analysis is a statistical method used to estimate the relationships between a dependent variable and one or more independent variables. It is commonly employed for prediction, forecasting, and inferring causal relationships. By analyzing the influence of independent variables on a dependent variable, regression analysis helps in understanding which factors are important and how these factors impact each other. It is widely used in various fields, including finance, marketing, and data analysis, to make informed decisions and gain valuable insights.

Fig 11: Regression

VII TUNNED DEEP LEARNING

A. PSO

PSO-LSTM refers to the combination of Long Short-Term Memory (LSTM) neural networks with Particle Swarm Optimization (PSO). This hybrid approach aims to optimize the LSTM model by using PSO to obtain the optimal parameters, thereby improving the accuracy of predictions in various applications. The use of PSO in conjunction with LSTM has been shown to enhance the performance of the LSTM model in tasks such as prediction, positioning control, and rainfall-runoff simulation, as evidenced by several research studies.

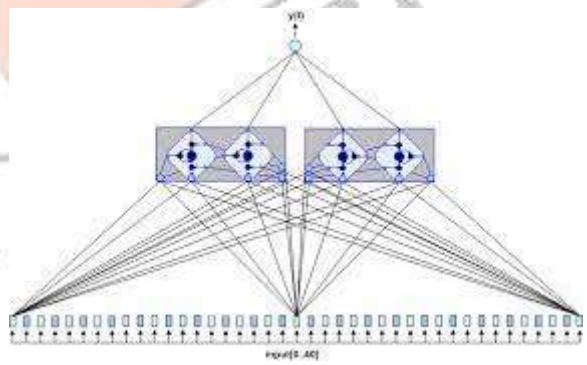


Fig 12: PSO-LSTM

B.POA

POA-LSTM refers to the combination of Long Short-Term Memory (LSTM) neural networks with Pastoralist Optimization Algorithm (POA). This hybrid approach aims to optimize the LSTM model by using POA to obtain the optimal parameters, thereby improving the accuracy of predictions in various applications. The use of POA in conjunction with

LSTM has been shown to enhance the performance of the LSTM model in tasks such as sentiment analysis, resource allocation in cloud environments, and prediction, as evidenced by several research studies.

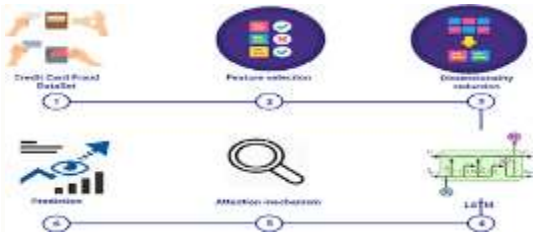
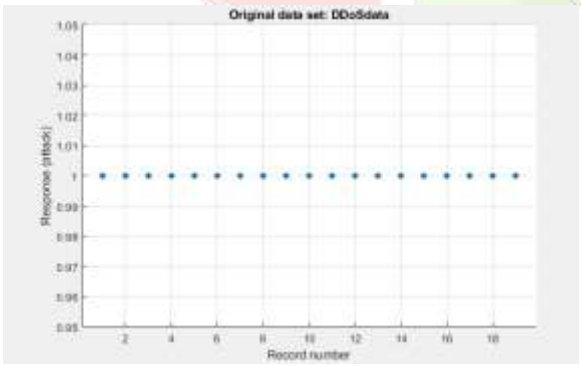


Fig13: POA-LSTM

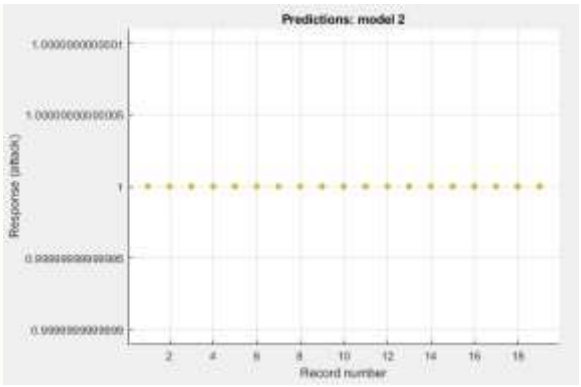
VIII ATTACK DETECTION

Attack detection is the process of identifying and preventing unauthorized access or activity in a network-based environment. This is achieved through the use of various techniques and tools, such as Attack Detectors, Presentation Attack Detection (PAD), State full Firewalls, and Dynamic Packet-Filtering Methods. These methods work together to enhance the security of networks and systems, ensuring that they remain protected from potential cyber threats and attacks.

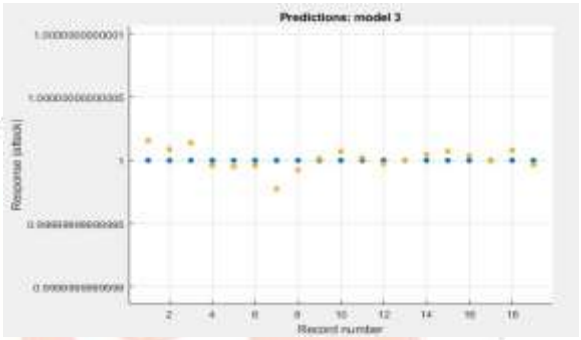
IX RESULT



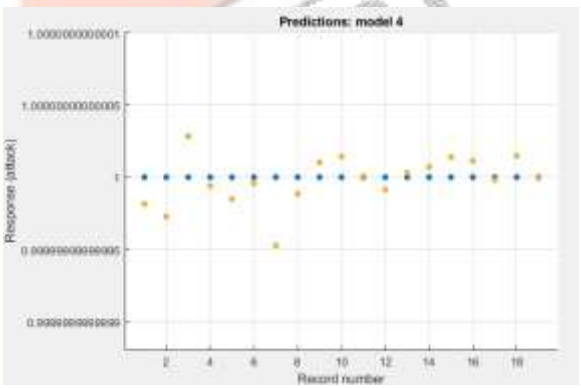
Fine Tree Method Graph



Rational Quadratic GPR Method Graph



Linear Method Graph



Linear Interaction Method Graph

REFERENCES

[1] S. Salini and B. P. U. Ivy, "Chapter 3 - digital twin and artificial intelligence in industries," in Digital Twin for Smart Manufacturing, R. K. Dhanaraj, A. K. Bashir, V. Rajasekar, B. Balusamy, and P. Malik, Eds. Academic Press, 2023, pp. 35–58. [Online]. Available: https: //www.sciencedirect.com/science/article/pii/B97803 23992053000146

[2] R. U. Rasool, H. F. Ahmad, W. Rafique, A. Qayyum, and J. Qadir, "Security and privacy of internet of medical things: A contemporary review in the age of surveillance, botnets, and adversarial ml," Journal of Network and Computer Applications, vol. 201, p. 103332, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/ S1084804522000017

[3] H. Benyezza, M. Bouhedda, R. Kara, and S. Rebouh, "Smart platform based on iot and wsn for monitoring and control of a greenhouse in the context of precision agriculture," Internet of Things, vol. 23, p. 100830, 2023. [Online]. Available: https: //www.sciencedirect.com/science/article/pii/S254266 0523001531

[4] B. Jovanovic, 2022. [Online]. Available: https://dataprot.net/statistics/ iot-statistics/

[5] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "A vision of iot: Applications, challenges, and opportunities with china perspective," IEEE Internet of Things Journal, vol. 1, no. 4, pp. 349–359, 2014.
[6] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637–646, 2016.

[7] Y. Lu and L. D. Xu, "Internet of things (iot) cybersecurity research: A review of current research topics," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2103–2115, 2019.

[8] G. L. Nguyen, B. Dumba, Q.-D. Ngo, H.-V. Le, and T. N. Nguyen, "A collaborative approach to early detection of iot botnet," Computers Electrical Engineering, vol. 97, p. 107525, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0 045790621004717

[9] U. Garg, S. Kumar, and M. Ghanshala, "Analysis and categorization of emotet iot botnet malware," in 2023 International Conference on Artificial Intelligence and Smart Communication (AISC), 2023, pp. 909– 914.

[10] S. Dange and M. Chatterjee, "Iot botnet: The largest threat to the iot network," Advances in Intelligent Systems and Computing, 2019. [Online]. Available: https://api.semanticscholar.org/CorpusID: 208125836

[11] P. Kumari and A. K. Jain, "A comprehensive study of ddos attacks over iot network and their countermeasures," Computers Security, vol. 127, p. 103096, 2023. [Online].