Develop and Implementing INET (NETWORK SECURITY)

V.AshaJincy
M.E, (Computer Science and Engineering),
Bethlahem Institute Of Engineering, Kanyakumari District.

Ms.Marly.G
Assistant Professor (Computer Science and Engineering)
Bethlahem Institute of Engineering, Kanyakumari District

Ms.R.P Shyni Vinse,
Assistant Professor (Computer Science and Engineering)
Bethlahem Institue of Engineering, Kanyakumari District

Dr.L.Femila,
Assistant Professor (Electronics and Communication Engineering)
St.Xaviers Catholic College of Engineering, Chunkankadai

Abstract: In the contemporary landscape of rapidly evolving technology and interconnected systems, the proposed project assumes critical importance in addressing the escalating threat of malicious cyberattacks. Traditional cybersecurity measures often fall short in dealing with the sophistication and diversity of modern cyber threats. Hence, the integration of cutting-edge technologies, such as Suricata IDS/IPS, and the use of Python automation, adds a layer of adaptability and responsiveness to the security framework. Moreover, the real-time monitoring capabilities facilitated by Suricata, coupled with the nimble automation provided by Python scripts, enable the system to swiftly identify and counteract potential threats. In a world where cyber threats are becoming more dynamic and sophisticated, the need for a robust and agile defense mechanism is paramount. By demonstrating the efficacy of this integrated approach, the paper not only contributes to the field of cybersecurity research but also provides practical insights for organizations and individuals seeking to fortify their network security. In essence, the project addresses the imperative need for proactive measures in the face of an ever-evolving cyber threat landscape, promoting resilience and ensuring the integrity and security of digital systems in today's world.

Keywords: IDS, IPS, Suricata, Runet

1.1 INTRODUCTION

Our project stems from the need for a robust cybersecurity system, drawing inspiration from proven practices observed in systems like Runet. The integration of Suricata Intrusion Detection and Prevention Systems (IDS/IPS), Python automation, and an Ubuntu operating system forms the core framework. This proactive security model aims to dynamically monitor and defend against emerging threats, providing a swift and effective response.

1.2 NETWORK SECURITY MODEL

The network security involves all tools, devices, strategies and activities which enterprises and organizations undertake to protect their networks, data and operations. An effective network security strategy must include the most effective set of tools for identification and reflection various threats and attacks. Creation of well thoughtout network security model will effectively help you in realization your network's security. The network security model (NSM) is a scheme that reflects the general plan and the policy of ensuring the network security, and usually includes all or some of the following seven layers in different modifications according to the specific company's needs

1.3 INTRUSION DETECTION SYSTEM

A system called an intrusion detection system (IDS) observes network traffic for malicious transactions and sends immediate alerts when it is observed. It is software that checks a network or system for malicious activities or policy violations. Each illegal activity or violation is often recorded either centrally using a SIEM system or notified to an administration. IDS monitors a network or system for malicious activity and protects a computer network from unauthorized access from users, including perhaps insiders. The intrusion detector learning task is to build a predictive model (i.e. a classifier) capable of distinguishing between 'bad connections' (intrusion/attacks) and 'good (normal) connections'.

An IDS (Intrusion Detection System) monitors the traffic on a computer network to detect any suspicious activity. It analyzes the data flowing through the network to look for patterns and signs of abnormal behavior. The IDS compares the network activity to a set of predefined rules and patterns to identify any activity that might indicate an attack or intrusion. If the IDS detects something that matches one of these rules or patterns, it sends an alert to the system administrator. The system administrator can then investigate the alert and take action to prevent any damage or further intrusion..

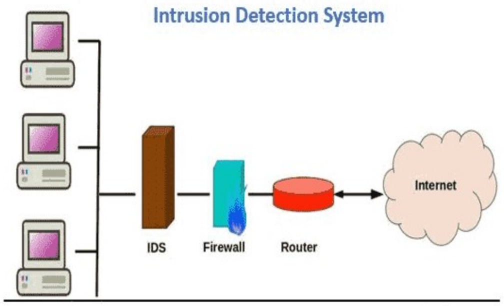

Fig 1.2: Intrusion Detection System

Benefits of IDS:

- Detects malicious activity: IDS can detect any suspicious activities and alert the system administrator before any significant damage is done.
- Improves network performance: IDS can identify any performance issues on the network, which can be addressed to improve network performance.

1.4 INTRUSION PREVENTION SYSTEM

Intrusion Prevention System (IPS) Intrusion Prevention System is also known as Intrusion Detection and Prevention System. It is a network security application that monitors network or system activities for malicious activity. Major functions of intrusion prevention systems are to identify malicious activity, collect information about this activity, report it and attempt to block or stop it. Intrusion prevention systems are contemplated as augmentation of Intrusion Detection Systems (IDS) because both IPS and IDS operate network traffic and system activities for malicious activity. IPS typically record information related to observed events, notify security administrators of important observed events and produce reports. Many IPS can also respond to a detected threat by attempting to prevent it from succeeding. They use various response techniques, which involve the IPS stopping the attack itself, changing the security environment or changing the attack's content. An IPS works by analyzing network traffic in real-time and comparing it against known attack patterns and signatures. When the system detects suspicious traffic, it blocks it from entering the network.

Need of IPS:

An IPS is an essential tool for network security. Here are some reasons why:

- Protection Against Known and Unknown Threats
- Compliance Requirements
- Cost-Effective
- Increased Network Visibility

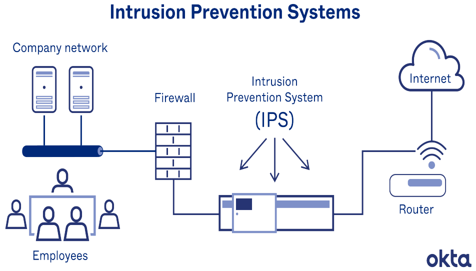

Fig1.3:Intrusion Prevention system

2.1 LITERATURE SURVEY

The literature review examines recent developments in the domain of network intrusion detection, with a primary focus on understanding and refining techniques for enhanced detection capabilities. Several noteworthy studies contribute valuable insights to this overarching theme, collectively aiming to bolster the efficiency and efficacy of network intrusion detection systems.

“Network intrusion detection using oversampling technique and machine learning algorithms.”- *Hafiza Anisa Ahmed, Anum Hameed,Narmeen Zakaria Bawany*

Hafiza Anisa Ahmed proposes a framework that leverages machine learning classification schemes to detect various types of network attack categories, enhancing overall security measures. However, the reliance on a dataset of known attack types may limit its effectiveness in detecting novel or evolving attack patterns not represented in the training data. To implement NIDS, a stream of supervised and unsupervised machine learning approaches is applied to detect irregularities in network traffic and to address network security issues. Such NIDSs are trained using various datasets that include attack traces. However, due to the advancement in modern-day attacks, these systems are unable to detect the emerging threats. Therefore, NIDS needs to be trained and developed with a modern comprehensive dataset which contains contemporary common and attack activities.

“Hybrid Intrusion Detection System For Detecting Internet Of Things Attacks”- *Ansam Khraisat, Iqbal Gondal,ET.Al*

This innovative approach combines both signature-based (SIDS) and anomaly-based (AIDS) intrusion detection systems to achieve higher accuracy in detecting known and unknown attacks. However, the evaluation using the BOT-IOT dataset might limit the generalizability of results to broader IoT contexts. The Internet of Things (IoT) has been rapidly evolving towards making a greater impact on everyday life to large industrial systems. Unfortunately, this has attracted the attention of cybercriminals who made IoT a target of malicious activities, opening the door to a possible attack to the end nodes. Due to the large number and diverse types of IoT devices, it is a challenging task to protect the IoT infrastructure using a traditional intrusion detection system. To protect IoT devices, a novel ensemble Hybrid Intrusion Detection System (HIDS) is proposed by combining a C5 classifier and One Class Support Vector Machine classifier.

“Novel Intrusion Detection System (IDS) for Internet of Things (IoT) devices and data, termed TLBO-IDS”- *Ajay Kaushik:*

The TLBO-IDS optimizes intrusion detection strategies to ensure optimal throughput in IoT networks, balancing effectiveness and efficient resource utilization. However, the complexity of the TLBO-IDS algorithm may pose challenges for less experienced users or developers, potentially limiting widespread adoption. As we enter the new age of the Internet of Things (IoT) and wearable gadgets, sensors, and embedded devices are extensively used for data aggregation and its transmission. The extent of the data processed by IoT networks makes it vulnerable to outside attacks. Therefore, it is important to design an intrusion detection system (IDS) that ensures the security, integrity, and confidentiality of IoT networks and their data. State-of-the-art IDSs have poor detection capabilities and incur high communication and device overhead, which is not ideal for IoT applications requiring secured and real-time processing.

“A New Ensemble-Based Intrusion Detection System for Internet of Things”- *Adeel Abbas, Muazzam A. Khan Khattak,ET.Al*

This model integrates logistic regression, naive Bayes, and decision tree algorithms through a voting classifier, showcasing improved accuracy in both binary and multi-class classification scenarios. The evaluation utilized the CICIDS2017 dataset, and the results indicated significant enhancements compared to existing state-of-the-art techniques. However, it's essential to consider the specific characteristics of the dataset used and recognize potential limitations in generalizing the findings to diverse IoT contexts. The domain of Internet of Things (IoT) has witnessed immense adaptability over the last few years by drastically transforming human lives to automate their ordinary daily tasks. This is achieved by interconnecting heterogeneous physical devices with different functionalities. Consequently, the rate of cyber threats has also been raised with the expansion of IoT networks which puts data integrity and stability on stake. In order to secure data from misuse and unusual attempts, several intrusion detection systems (IDSs) have been proposed to detect the malicious activities on the basis of predefined attack patterns.

2.2 EXISTING SYSTEM

"Runet" refers to the Russian-language segment of the internet, encompassing the digital space used predominantly by Russian speakers. The term "Runet" is a combination of "Russia" and "Internet." The Russian government has a significant role in regulating and controlling online activities within Runet. This includes implementing laws and measures to ensure national security and combat cyber threats. However, some of these measures have raised concerns about privacy and freedom of expression. Russia has taken steps to increase its digital sovereignty, aiming to have more control over the digital infrastructure within its borders. The "sovereign internet" law, for example, allows the government to isolate the country's internet infrastructure from the global network under certain circumstances. Russia has introduced the "sovereign internet" law, which grants the government the authority to control and regulate internet traffic within its borders. This law allows for measures such as the isolation of the Russian internet from the global network in case of perceived threats. Concerns have been raised about surveillance practices within Runet. The government's access to user data and communications for security purposes has implications for privacy rights. These concerns are part of broader discussions about balancing national security with individual privacy. Runet is not immune to the global cybersecurity landscape. Russian-speaking users and organizations face threats such as hacking, malware, phishing, and other cyber attacks. The government and private entities within Runet are actively involved in cybersecurity efforts to mitigate these threats.

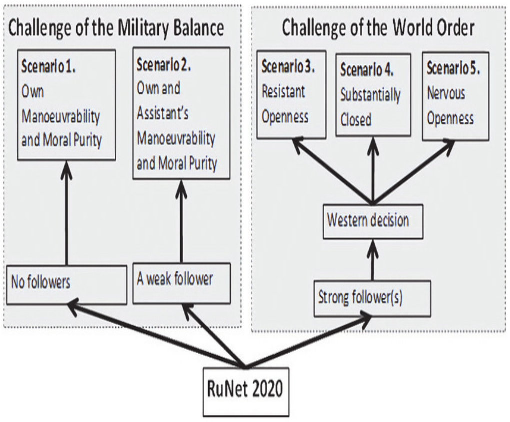
Challenge of the Military Balance
Challenge of the World Order
Scenario 1. Own Manoeuvrability and Moral Purity
Scenario 2. Own and Assistant's Manoeuvrability and Moral Purity
Scenario 3. Resistant Openness
Scenario 4. Substantially Closed
Scenario 5. Nervous Openness
Western decision
No followers
A weak follower
Strong follower(s)
RuNet 2020

Figure 2.1: Existing block diagram

2.3 DRAWBACKS

- Complexity

❖ The scenarios exhibit complexity in their attributes and interactions.

❖ Disconnecting from the global internet could isolate Russia from the vast pool of global information.

- Increased Storage Requirements:

4.1 PROPOSED SYSTEM

In response to the escalating threat of malicious cyberattacks, this project introduces a proactive security model inspired by Runet. Leveraging Suricata IDS/IPS and Python programming on the Ubuntu OS, the system dynamically monitors and defends against threats. Suricata serves as the primary defense, inspecting network traffic for malicious activities. Python scripts complement Suricata by monitoring real-time logs. Upon detecting a threat, the system initiates an automated response, blocking the source IP and isolating the destination IP using Python scripting. Operating on Ubuntu ensures a stable environment for these cybersecurity measures. The project aims to demonstrate the efficacy of an integrated approach, combining cutting-edge IDS/IPS capabilities with Python automation, to fortify network security and respond swiftly to emerging cyber threats.

4.2 MODULES OF ARCHITECTURE

➢ Threat Identification and Response Module

➢ System Stability Module

4.2.1 Threat Identification and Response Module:

This module involves the proactive identification of threats through Suricata IDS/IPS. Python scripts are then employed to monitor real-time logs, enabling automated responses to detected threats. The system initiates actions such as blocking the source IP and isolating the destination IP upon threat detection.

4.2.2 System Stability Module:

Operating on the Ubuntu OS ensures system stability, providing a reliable and robust environment for the cybersecurity measures. This module emphasizes the importance of a stable operating system in supporting the effectiveness of the integrated security approach.

4.3 SYSTEM STABILITY MODULE

4.3.1 Ubuntu OS as the Stable Foundation

The choice of the Ubuntu operating system provides a stable foundation for the entire cybersecurity infrastructure. Ubuntu's robust security features, regular updates, and extensive community support contribute to a secure and reliable environment. This module ensures that the cybersecurity measures operate within a stable framework, minimizing vulnerabilities and potential points of failure.

5. CONCLUSION

In conclusion, our cybersecurity project represents a comprehensive and proactive approach to safeguarding digital assets in the dynamic landscape of cybersecurity. The integration of Suricata IDS/IPS, Python automation, and the stable Ubuntu operating environment forms a robust defense model against emerging threats. Real-time threat monitoring, automated response mechanisms, and simulations like ARP spoofing contribute to the project's efficacy in minimizing the impact of security incidents. The significance of an integrated approach is underscored by the successful synergy between cutting-edge IDS/IPS capabilities and Python automation. This model enhances adaptability, making our cybersecurity solution well-equipped to handle diverse and evolving cyber threats. The choice of Ubuntu as the operating system provides a stable and standardized platform, ensuring reliability and consistency in implementing cybersecurity measures.

REFERENCES

[1] S. S. Malik, V. K. Shukla, A. Mishra, and S. Tiwari, "Design of a Low-Cost IoT-based Gas Leakage Monitoring System," 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), 2020.

[2] A. Kumar, A. P. Shukla, S. Kumari, and R. Singh, "IoT-Based Gas Leakage Detection System for Smart Cities," 2019 International Conference on Communication and Signal Processing (ICCSP), 2019.

[3] P. Sharma, S. Gupta, A. Kumar, and S. K. Bhandari, "Wireless Sensor Network for Gas Leakage Detection and Monitoring," 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2018.

[4] M. S. Khan, M. I. Y. Essa, M. H. Alhussein, and M. E. Al-Kuhaili, "Development of Gas Leakage Detection and Alerting System Using IoT," 2017 IEEE International Conference on Electro/Information Technology (EIT), 2017.

[5] "LPG/CNG Gas Leakage Detection System with GSM Module" by Alan M John, Bhavesh Purbia, Ankit Sharma, Mrs.A.S Udapurkar in International Journal of Advanced Research in Computer and Communication Engineering, Vol. 6, Issue 5,May 2017

[6] C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of ELECTRICAL ENGINEERING, Vol.63 (6), pp.365-372, Dec.2012.

[7] C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011.

[8] C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor &amp; Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011.

[9] C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.

[10]Nagarajan C., Neelakrishnan G., Akila P., Fathima U., Sneha S. "Performance Analysis and Implementation of 89C51 Controller Based Solar Tracking System with Boost Converter" Journal of VLSI Design Tools & Technology. 2022; 12(2): 34–41p.

[11]C. Nagarajan, G.Neelakrishnan, R. Janani, S.Maithili, G. Ramya "Investigation on Fault Analysis for Power Transformers Using Adaptive Differential Relay" Asian Journal of Electrical Science, Vol.11 No.1, pp: 1-8, 2022.

[12]G.Neelakrishnan, K.Anandhakumar, A.Prathap, S.Prakash "Performance Estimation of cascaded h-bridge MLI for HEV using SVPWM" Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:750-756

[13]G.Neelakrishnan, S.N.Pruthika, P.T.Shalini, S.Soniya, "Perfromance Investigation of T-Source Inverter fed with Solar Cell" Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:744-749

[14]C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007

[15]M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022

[16]M Suganthi, N Ramesh, CT Sivakumar, K Vidhya, "Physiochemical Analysis of Ground Water used for Domestic needs in the Area of Perundurai in Erode District", International Research Journal of Multidisciplinary Technovation, pp: 630-635, 2019.

[17] "LPG leakage detection and prevention system with GSM alert" by Swapnil Kadam, Sumit More, Prathamesh Borkar, Ritesh Gailwad, Prof. Prachi Gadhire in International Research Journal of Engineering and Technology (IRJET), Volume: 05 Issue: 03, Mar-2018.

[18] "A security alert system using GSM for gas eakage" by S.Rajitha, T.Swapna in International Journal of VLSI and Embedded Systems-IJVES, Vol 03, Issue 04; September- October 2012.

[19]"LPG Gas Weight and Leakage Detection System Using GSM" by Mr.Sameer Jagtap , Prajkta Bhosale, Priyanka Zanzane , Jyoti Ghogare in International Journal for Research in Applied Science & Engineering Technology (IJRASET), Volume 4 Issue III, March 2016.

[20]"Home and Industrial Safety IoT on LPG Gas Leakage Detection and Alert System" by Zainal H. C. Soh , Syahrul A. C. Abdullah , Mohd A. Shafie and Mohammad N. Ibrahim in Int. J. Advance Soft Compu. Appl, Vol. 11, No. 1, March 2019.

[21] "GSM BASED GAS LEAKAGE DETECTION SYSTEM" by Ashish Shrivastava, Ratnesh Prabhaker, Rajeev Kumar and Rahul Verma in International Journal of Technical Research and Applications, Volume 1, Issue 2 (may-June 2013).

[22] R. Gupta, A. Srivastava, and R. Gupta, "An IoT-Based Smart Gas Monitoring and Alerting System," 2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2016.