Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Special Issue 4, April : 2024

TWO FACTOR WORM DETECTION USING SIGNATURE AND ANOMALY

P Rajasekhar1, P Laxmi Sai2, K Priyanka3, M Vyshnavi 4, L Akshara 51,2,3,4,5 Department of Computer Science and Engineering, Vignan's Institute of Engineering for Women, Visakhapatnam, Andhra Pradesh, India

ABSTRACT
In the realm of Cyber Security, the detection of worms remains a crucial challenge due to their rapid propagation and ability to cause widespread damage. This project proposes a novel approach to enhance the efficacy of worm detection systems by leveraging both signature-based and anomaly-based techniques. The proposed system aims to bolster the accuracy and efficiency of worm detection in network environments. Signature based systems excel in identifying known worm patterns, they struggle with "zero-day attacks" and "polymorphic worms". Anomaly based systems detect deviations from normal behavior, but might produce high false positive and high false negative rates. By combining the strengths of both techniques, the system enhances detection accuracy by using Machine Learning algorithms like Random Forest and Decisio tree, while mitigating the limitations of individual methods. This synergistic approach for more robust and adaptable worm detection capabilities, effectively addressing both known and emerging threats.

Keywords: Anomaly detection, Signature detection,Intrusion Detection System.

INTRODUCTION

This paper presents a unique method for identification and classification of worms in network by combing both anomaly and signature based detection.Worms are malicious software entities programmed to self-replicate and spread throughout computer networks,pose formidable threats with far-reaching impacts. Their ability to propagate independently, exploiting network vulnerabilities, can lead to bandwidth congestion, system degradation, and compromise of sensitive data, imperiling both individual users and organizations.A robust defense strategy against worm attacks combines anomaly detection, which scrutinizes network behavior for deviations from norms, and signature-based detection, which identifies known worm patterns. Advanced classification algorithms like Random Forest and Decision Trees enhance accuracy. This synergy ensures swift detection, precise classification, and effective mitigation, safeguarding network integrity.

LITERATURE SURVEY

Reference: [1] ong Tang Shigang Chen Department of Computer & Information Science & Engineering University of Florida, "Defending Against Internet Worms: A Signature-Based Approach" Gainesville. FL 3261 1-6120, IEEE

Mainly focused on identification of polymorphic worms "Defending Against Internet Worms: A Signature- Based Approach" [1].

A novel double-honeypot system is deployed in a local network for automatic worm attack detection, isolating attack traffic from normal traffic. It triggers warnings and records ongoing worm instances. Polymorphic evasion techniques are addressed, with a focus on a new position-aware distribution signature (PADS) for detecting certain types of polymorphic worms. PADS offers flexibility beyond fixed string signatures and precision surpassing position-unaware statistical signatures, enhancing detection accuracy against evolving threats.

Reference: [2] Mohd Fadzli Marhusin1 , Chris Lokan1 , Henry Larkin2 , David Cornforth3 “A Data Mining Approach for Detection of Self-Propagating Worms” 1 University of New South Wales, ACT 2600, Australia 2 University of Aizu, Japan research@logic.nu 3 CSIRO Energy Technology, May field West NSW 2304, IEEE
Mohd Fadzli Marhusin1 , Chris Lokan , Henry Larkin , David Cornforth they are showcasing a signature-based detector for self-propagating worms, utilizing worm and benign traffic traces to construct profiles arranged into separate trees. Additionally, they demonstrate an anomaly detector to handle tied matches between worm and benign trees. Results indicate the signature-based detector achieves high true positives, while the anomaly detector addresses tied matches. Independently, both detectors suffer from high false positives, but integration maintains a high true positive detection rate and minimizes false positives.
Reference: [3]“Network Anomaly Detection Based on Statistical Approach and Time Series” Analysis Huang Kai School of software engineering Shanghai Jiao Tong University Shanghai, China, Qi Zhengwei School of software engineering Shanghai Jiao Tong University Shanghai, China Liu Bo School of software engineering Shanghai Jiao Tong University Shanghai, China. [3], . In our approach, we adapt the Gaussian

Mixture Model to approximate the combined statistical model. The Gaussian Mixture Model can be a model with less residual in the network distribution of combined traffic of different type. Then we use the EM algorism to estimate the value of different Gaussian distribution. We use the sum of all the value to evaluate the fluctuation of the network traffic. If a great change happened in a short time slot, an alarm will be triggered. We adapted two approaches to decide how great the change is and when to trigger an alarm. The first approach defines an up bound and low bound of the value. If the sum of all the values passes the bound, an alarm will be triggered. The second approach uses the historical mean value of the sum in a time slot to draw two lines with one more sensitive to the change of the new coming data. If the more sensitive one pass through the anther an alarm will be triggered.
Reference: [4] Suleiman Mohamed Ali Sulieman, Yahia A. Fadlalla,"Detecting Zero-day Polymorphic Worm: A Review", 2018 21st Saudi Computer Society National Computer Conference (NCC), pp.1-7, 2018. zero-day polymorphic worms, highlighting their elusive nature and threat to network security. It discusses the evolution of computer and network security, emphasizing the rise of automated tools facilitating attacks and the challenges posed by sophisticated threats like polymorphic worms. The paper delves into network protocols, security principles (CIA: Confidentiality, Integrity, Availability), and common network threats such
as viruses, eavesdropping, and worms. It provides insights into the components and behavior of worms, including reconnaissance, exploitation, propagation, payload, and concealment techniques.
EXISTING METHOD
The existing system for worm detection in cybersecurity consists of two primary techniques: signature-based and anomaly-based systems. Signature-based systems operate by matching incoming network traffic against a database of known worm signatures or patterns, effectively identifying previously identified worms but struggling with zero-day attacks or polymorphic worms. On the other hand, anomaly-based systems monitor network traffic for deviations from established baseline behavior, successfully detecting novel or zero-day attacks but often resulting in high false positive rates due to legitimate activities appearing anomalous. Each method offers unique advantages, yet neither alone provides comprehensive protection against the wide range of worm threats in network environments.
Drawbacks:

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Special Issue 4, April : 2024

1. Limited Signature Coverage: Signature-based detection relies on known patterns, making it ineffective against zero-day exploits or new worm variants.
2. False Positives: Signature-based detection can trigger alarms for benign activities resembling known malicious signatures, leading to wasted resources.
3. Signature Maintenance Overhead: Updating signature databases to keep pace with evolving malware is resource-intensive and may lag behind emerging threats.
4. Limited Anomaly Detection Accuracy: Anomaly detection can misclassify legitimate activities as malicious, requiring careful tuning to balance false positives and sensitivity.
5. Resource Intensive: Anomaly detection demands significant computational resources, potentially causing performance issues or necessitating costly hardware.
6. Detection Latency: Both detection methods may suffer from delays in recognizing threats, allowing worms to propagate and cause damage before mitigation.
7. Evasion Techniques: Worm authors can employ evasion tactics like polymorphic code or encryption to evade detection, challenging both signature-based and anomaly systems.
8. Scalability Issues: As network traffic grows, scalability becomes a concern, necessitating additional resources to maintain timely and accurate detection across large-scale networks.

PROPOSED METHOD

The proposed system aims to enhance the efficacy of worm detection in network environments by integrating both signature-based and anomaly-based techniques. This approach seeks to bolster detection accuracy and efficiency while mitigating the limitations of individual methods. Signature-based systems, known for their proficiency in identifying known worm patterns, excel in detecting previously identified threats such as Code Red, Slammer, Nimda, and Witty. They struggle with zero-day attacks and polymorphic worms. Conversely, anomaly-based systems detect deviations from normal behavior, effectively identifying novel or zero-day attacks but may produce high false positive and high false negative rates. By combining the strengths of both techniques and leveraging machine learning algorithms such as Random Forest and Decision Trees, the proposed system aims to achieve more robust and adaptable worm detection capabilities. This synergistic approach is anticipated to effectively address both known and emerging threats, thereby enhancing the overall security posture of network environments against worm propagation.

SYSTEM ARCHITECTURE

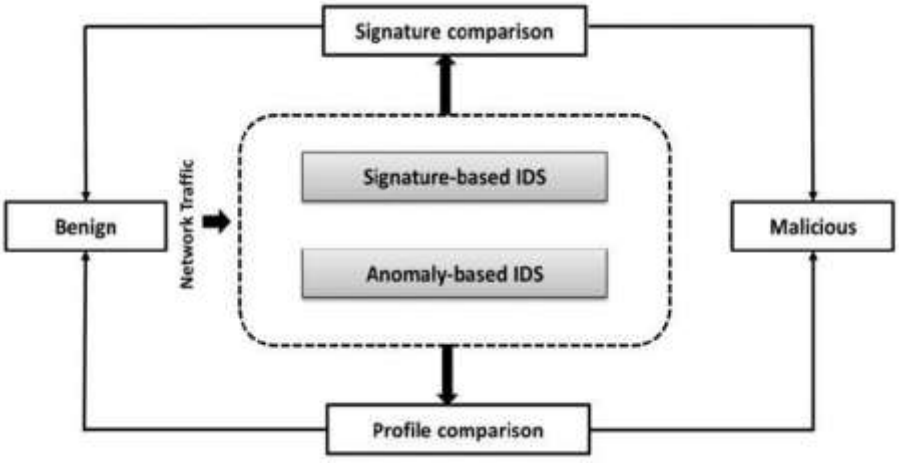

Fig 1: Implementation of Signature and Anomaly Detection

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Special Issue 4, April : 2024

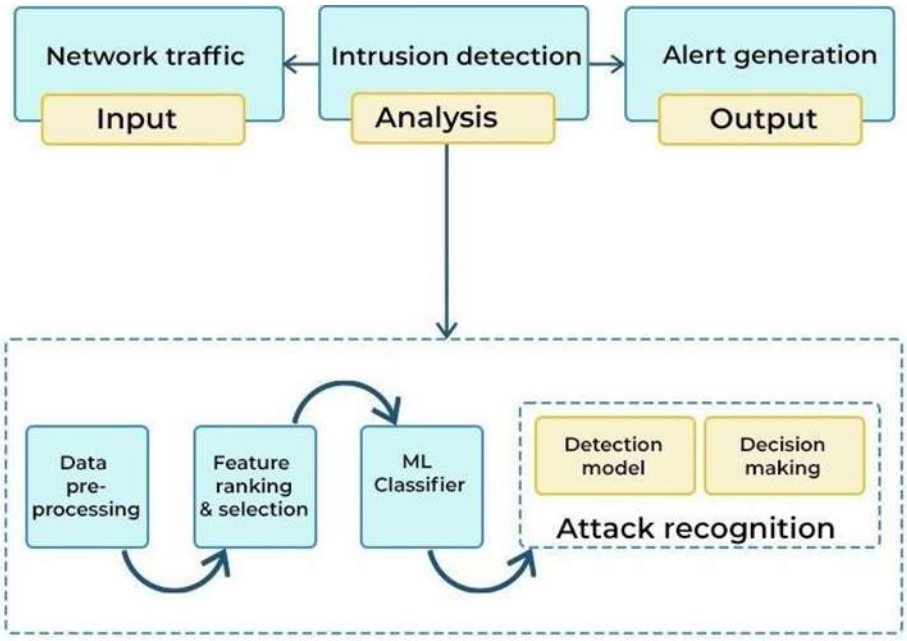

Fig 2: Implementation of ML algorithms to classify attacks

OUTPUT SCREENS:

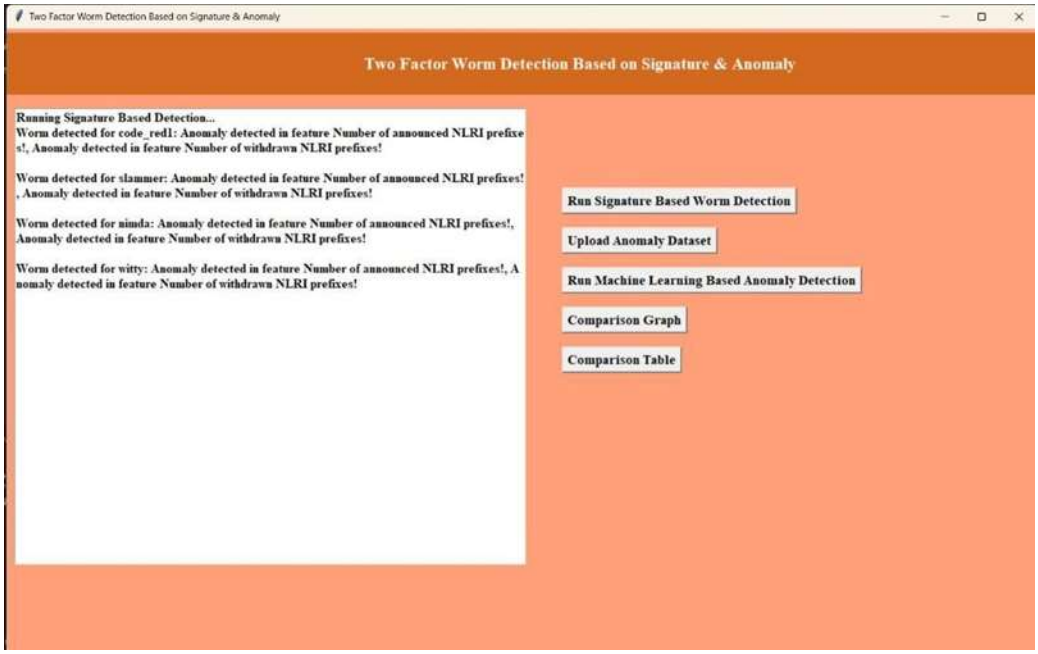

Fig 3: Signature based detection of worms

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Special Issue 4, April : 2024

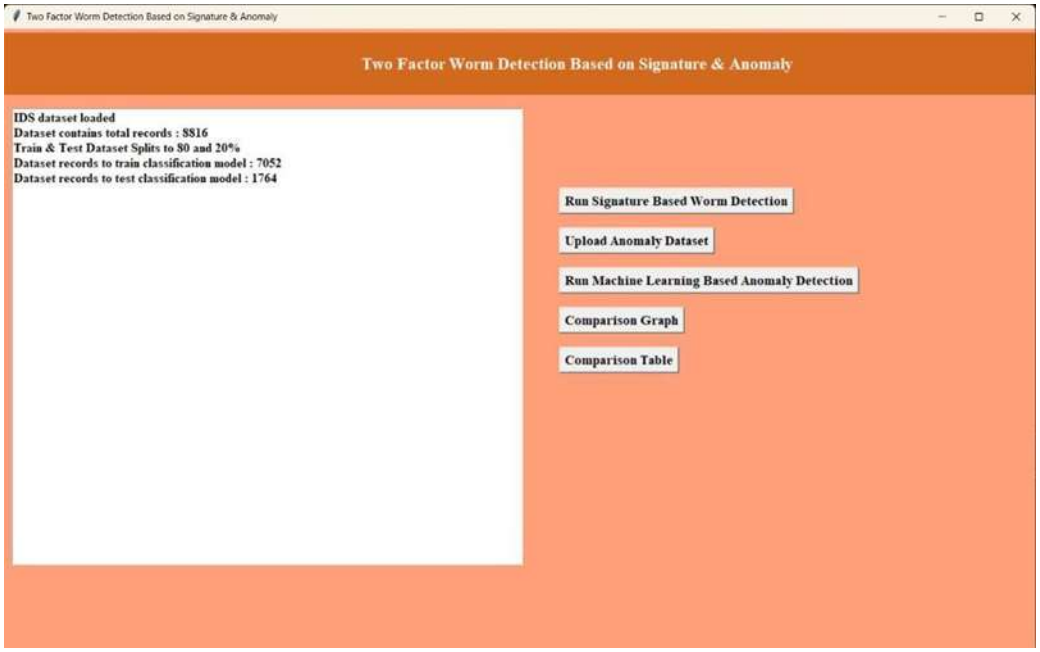

Fig 4. Anomaly Dataset uploaded

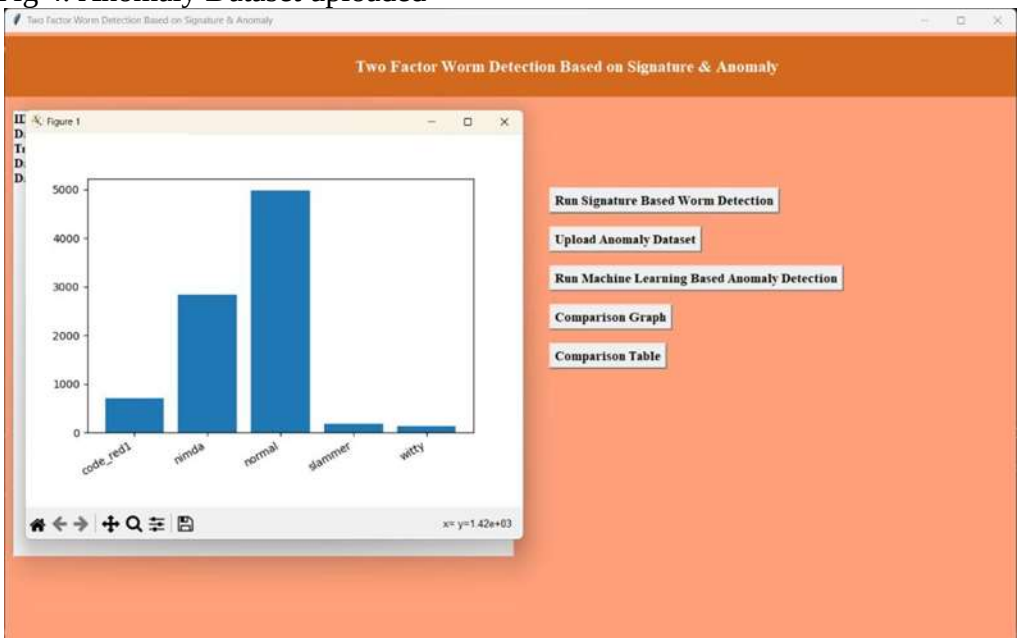

Fig 5- Representation of worms

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Special Issue 4, April : 2024

Fig 6- Prediction Accuracy of Machine Learning Techniques

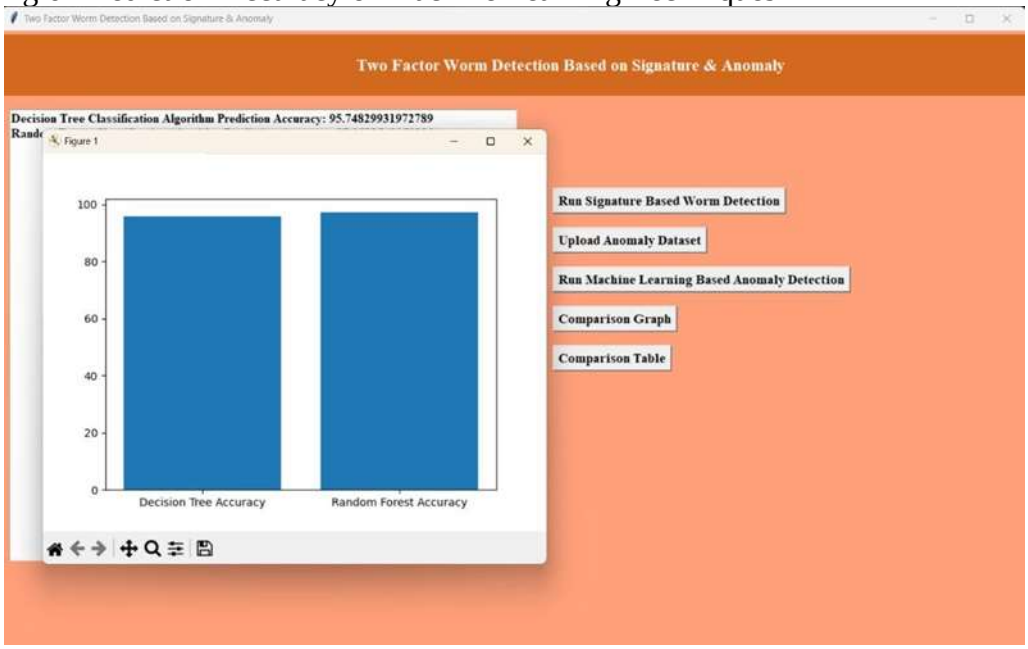

Fig 7- Comparision Graph

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Special Issue 4, April : 2024

Fig 8 -Comparision Table

CONCLUSION

In conclusion, Integration of both Signature and Anomaly-based techniques within the proposed Two-Factor Worm Detection framework presents a promising solution to bolster internet security against malicious worm attacks.Through the utilization of machine learning algorithms such as Decision Trees, Random Forests, and coupled with the analysis of internet traffic signatures and anomaly detection in network behavior, the system achieves a multi- layered defense strategy.With regards to accuracy, the system demonstrates notable performance. The Signature-based detection method showcasing its efficacy in identifying known worm signatures within network traffic. Similarly, the Anomaly-based detection utilizing machine learning models achieves an impressive accuracy of up to 96%, enabling the system to predict and mitigate abnormal traffic behaviors indicative of worm attacks.By combining these methodologies, the proposed system offers a comprehensive approach to worm detection, addressing both known and unknown threats effectively.In essence, the proposed Two-Factor Worm Detection system not only enhances internet security but also contributes to the preservation of network integrity, safeguarding both individual users and organizations against the detrimental impacts of worm attacks

REFERENCES

[1] R. Kaur and M. Singh, ‘‘A survey on zero-day polymorphic worm detection techniques,’’ IEEE Commun. Surveys Tuts., vol. 16, no. 3, pp. 1520–1549, 3rd Quart., 2014.

[2] Fangwei Wang, Shaojie Yang, Dongmei Zhao, Changguang Wang, "An Automatic Signature-Based Approach for Polymorphic Worms in Big Data Environment", 2019 International Conference on Networking and Network Applications (NaNA), pp.223-228, 2019.

[3] Suleiman Mohamed Ali Sulieman, Yahia A. Fadlalla, "Detecting Zero-day Polymorphic Worm: A Review", 2018 21st Saudi Computer Society National Computer Conference (NCC), pp.1-7, 2018.

[4] Fangwei Wang, Shaojie Yang, Changguang Wang, Qingru Li, Kehinde O. Babaagba, Zhiyuan Tan,"Toward machine intelligence that learns to fingerprint polymorphic worms in IoT", International Journal of Intelligent Systems, vol.37, no.10, pp.7058, 2022.

[5] T. Ahmed, B. Oreshkin, and M. Coates, “Machine learning approaches to network anomaly detection,”
C. M. Bishop, Pattern Recognition and Machine Learning. Secaucus, NJ, USA: Springer-Verlag, 2006.

[6] A. L. Buczak and E. Guven, “A survey of data mining and machine learning methods for cyber security intrusion detection,” IEEE Commun. Surv. Tut.,, vol. 18, no. 2, pp. 1153–1176, 2016.

[7] V. Chandola, A. Banerjee, and V. Kumar, “Anomaly detection: a survey,” ACM Comput. Surv., vol. 41, no. 3, pp. 15:1–15:58, July 2009.