ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

DUAL FACTOR WORM DETECTION BASED ON SIGNATURE AND ANOMALY

[1]D. LAKSHMAN BABU , [2]K.Sai Kiran, [3]K.Sai Vardhini,[4] Ch.Raghavendra, [5]N.Arjun

[1]Assistant Professor in Department of Artificial Intelligence and Data Science Nalla Malla Reddy Engineering College

[1]lakshmanbabu.l@gmail.com

[2,3,4,5] UG Scholars in Department of Artificial Intelligence and Data Science Nalla Malla Reddy Engineering College

ksaikiran950@gmail.com, vardhini3030@gmail.com, chitikenraghavendra@gmail.com , Narlaarjun4@gmail.com

Abstract

Internet worms pose a major threat to computer systems, spreading rapidly and causing widespread disruption. To effectively combat these threats, a comprehensive and multi-layered detection strategy is crucial. This paper introduces a dual-method detection system that combines signature-based and anomaly-based techniques for enhanced security. Signature-based detection works by analyzing network traffic against a database of known worm signatures, allowing security systems to recognize malicious patterns through pattern matching. This approach involves inspecting PCAP files, enabling network administrators to detect unusual activities and potential security breaches. Honeypot-based detection takes a proactive approach by deploying decoy systems designed to attract and trap malicious attackers. By examining the logs generated from these honeypots, security professionals can pinpoint compromised systems and uncover potential attack methods. NetFlow-based detection, on the other hand, utilizes network flow data to monitor traffic patterns, identifying irregularities that deviate from typical network behavior. By analyzing these flow records, security teams can detect suspicious activities that may indicate worm propagation. Additionally, machine learning-based anomaly detection techniques—leveraging models such as Random Forest, Decision Trees, and Bayesian Networks—enhance the system's ability to recognize deviations from normal network behavior. By training these models on historical network data, security analysts can identify new and evolving threats that traditional signature-based detection might overlook.By integrating these complementary methods, this system strengthens worm detection capabilities, ensuring better protection against both known and emerging cyber threats. This approach plays a crucial role in mitigating risks, preserving network security, and safeguarding critical infrastructure.

Keywords: Two-Phase Worm Detection System, Signature-Based Approach, Anomaly-Based Technique, PCAP Files, Random Forest, Decision Tree, Bayesian Networks.

I. INTRODUCTION

the contemporary digital landscape, safeguarding computer networks from the menace of internet worms is imperative to ensure data integrity and user security. Our project focuses on enhancing the efficiency and reliability of worm detection through a comprehensive Two Factor authentication system that incorporates both

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

Signature and Anomaly detection techniques. Internet worms, malicious programs downloaded onto users' computers through online channels, have the potential to corrupt files and compromise user information, posing significant cybersecurity threats. In response to these challenges, our project leverages advanced detection methodologies to fortify network defenses and thwart potential cyberattacks. This method involves identifying worms by comparing their characteristics, known as signatures, with a database of known worm signatures. If a match is found, the system flags it as a worm. However, this method may miss new, unknown worms.This approach focuses on detecting deviations from normal network behavior. It establishes a baseline of regular activity and flags any unusual patterns that may indicate a worm attack. It's effective against new, unidentified worms but can generate false positives. Combining both methods creates a robust defense system. Signature-based detection catches known threats, while anomaly-based detection helps identify novel or evolving worm attacks. Web worms keep on compromising client information and security, making compelling location essential. We utilize a few high-level strategies to accomplish this objective. To begin with, our Mark Based Recognition investigates web traffic marks against predefined rules utilizing parcel catch (PCAP) documents, empowering continuous ID of vindictive traffic. Our framework conducts NetFlow-Based Examination by reviewing UDP and TCP marks to observe typical from assault marks. Finally, we utilize Irregularity Identification Models, which are prepared on authentic datasets utilizing AI calculations, for example, Arbitrary Woodland, Choice Tree, and Bayesian Organizations, to recognize strange traffic conduct..

Network safety dangers endure as an imposing test in the present interconnected world. As time passes, foes devise modern strategies to invade networks, compromising delicate data and basic foundation. Customary strategies for safeguard, especially in parcel based assault recognition, frequently battle to stay up with the unique idea of these dangers. This highlights the squeezing need for inventive and versatile ways to deal with brace network security. This undertaking presents a clever technique that amalgamates signature-based and inconsistency based recognition frameworks to defy the intricacies of recognizing parcel based assaults. Signature-put together frameworks work with respect to predefined designs and known assault marks, offering productivity in perceiving natural dangers. Nonetheless, their adequacy decreases when confronted with novel or changed assault designs. Then again, irregularity based frameworks examine deviations from laid out standards, alarming potential dangers that don't adjust to run of the mill conduct. However, they wrestle with high misleading positive rates, obstructing exact danger ID. Because of these difficulties, this undertaking use AI calculations — explicitly Choice Trees, Arbitrary Woods, and Gaussian NB

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

— to enable the recognition framework. By coordinating these calculations, the point is to support precision and proficiency in distinguishing and classifying bundle based assaults. This exploration attempts to contribute altogether to the network safety space by investigating the expected cooperative energy between signature-based and oddity based approaches. The goal is to make a hearty and versatile guard system fit for relieving developing digital dangers. The discoveries expect to advise the improvement regarding progressed recognition frameworks, offering upgraded security for networks against the consistently developing scene of digital dangers. This mark based approach is especially important for recognizing realized assault designs continuously, giving a prompt reaction to possible dangers. Supplementing the mark based approach, our framework consolidates Inconsistency.

II. LITERATURE SURVEY

worm detection system based on deep learning

In the study, the author utilizes Convolutional Neural Networks (CNNs) and Recurren tNeuralNetworks (RNNs) to model and analyze network traffic data. These deep learning architectures are chosen for their ability to learn complex patterns and features from vast amounts of data, making them well-suited for detecting anomalies indicative of worm activity. Data collection for the study involves both simulated network traffic and real-world datasets to ensure robust model training and validation. Preprocessing steps such as normalization and feature extraction are crucial for preparing the data for deep learning algorithms. The author details the training process, including hyperparameter tuning and the use of validation datasets to optimize model performance.

Zero-Day Polymorphic Worm Detection Techniques

These worms exploit zero-day vulnerabilities, making them particularly dangerous. Traditional signature-based detection methods are often ineffective, as polymorphic worms modify their appearance. Heuristic-based detection analyzes unusual system behavior, while anomaly-based detection establishes a baseline of normal activity to identify deviations indicative of an attack. Static and dynamic analysis techniques help understand the characteristics One effective approach is heuristic-based detection, which assesses behavior rather than relying solely on known signatures. By monitoring system activities and identifying anomalies, this method can flag potential infections from polymorphic worms. Similarly, anomaly-based detection establishes a baseline of normal network behavior, enabling the identification of unusual patterns that may indicate a zero-day attack.Static analysis examines the worm's code without executing it, looking for vulnerabilities or suspicious patterns. In contrast, dynamic analysis involves executing the code in a controlled

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

environment, observing its behavior in real-time. This dual approach provides comprehensive insights into the characteristics of polymorphic worms.Machine learning techniques play a crucial role in enhancing detection capabilities. By leveraging algorithms that learn from vast datasets, these methods can identify patterns and features associated with zero-day threats, adapting to new variants over time. This adaptability is vital, as attackers continuously modify their tactics.Behavioral analysis further strengthens detection efforts by monitoring system calls, file access patterns, and network traffic.

Graph based signature classes for detecting polymorphic worms via content analysis

Graph-based signature classes for detecting polymorphic worms through content analysis offer a promising approach to enhance cybersecurity. By representing polymorphic worms asgraphs—where nodes correspond to code elements and edges denote relationships—this method captures the structural characteristics of malware. Signature classes are formed by clustering similar graph structures, allowing for unique signatures that can identify various worm variants. Content analysis examines the actual code and behavior, enabling the detection system to compare new samples against established signatures. Integrating dynamic analysis further improves detection by updating graph models based on observed behaviors. This approach reduces false positives by focusing on structural similarities rather than exact matches. Additionally, graph traversal algorithms facilitate efficient comparison of new samples, enhancing detection speed.

Detecting intra-enterprise scanning worms based on address resolution

Detecting intra-enterprise scanning worms based on address resolution focuses on identifying malicious activities within a network. These worms often exploit vulnerabilities by scanning IP addresses to locate potential targets. By analyzing address resolution protocols, such as ARP (Address Resolution Protocol), security systems can monitor unusual patterns indicative of scanning behavior. This method enhances **detection capabilities**

III. EXISTING SYSTEM

The modern cybersecurity landscape employs a variety of techniques to detect and mitigate internet worms. Signature-based detection plays a crucial role by analyzing network traffic and comparing it against predefined rules using PCAP files, making it possible to identify known malicious patterns. Another widely used method is honeypot-based detection, where decoy servers are deployed to attract and log malicious activity, providing security teams with valuable insights into attack strategies and system vulnerabilities. NetFlow-based detection further enhances security by monitoring network traffic and analyzing UDP and TCP signatures to identify unusual activity patterns. In addition, anomaly

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

detection models, powered by machine learning algorithms trained on historical datasets, help detect deviations from normal network behavior, enabling the identification of emerging threats.

Despite these advancements, there are still challenges in improving detection accuracy, real-time responsiveness, and adaptability to ever-evolving cyber threats. Strengthening these aspects remains essential for developing more resilient cybersecurity frameworks.

Limitations of the Existing System

Implementing both signature

based and anomaly - based detection systems can be resource -intensive in terms of processing power and storage requirements. Anomaly detection, in particular, may need continuous monitoring and analysis of network traffic, which can strain resources.

• Managing and fine - tuning two detection methods simultaneously can introduce complexity. It may require expertise to configure and maintain both systems effectively, potentially leading to increased operational overhead. While anomaly detection helps reduce false positives compared to signature -based detection alone, it can still generate false alarms due to legitimate but unusual network activities.

• Balancing between false positives and false negatives can be a challenge. Sophisticated worms that are designed to evade signature detection or mimic normal behavior closely can sometimes bypass both signature and anomaly detection methods. In such cases, relying solely on these two factors may not be sufficient.

IV . PROBLEM STATEMENT

Given the limitations of existing authentication mechanisms, there is a need for a lightweight yet robust dual-factor authentication framework that ensures:

- **High Security:** Protection against replay attacks, MITM attacks, and brute-force attempts.
- **Low Computational Overhead:** Optimized encryption mechanisms for seamless deployment in IoT environments.
- **Fast Authentication Time:** Real-time usability without excessive processing delays.

V. PROPOSED SYSTEM

proposed Two Factor Worm Detection system combines the strengths of Signature and Anomaly detection techniques.

In Signature-based detection, we utilize PCAP datasets to analyze internet traffic signatures. Simultaneously, Anomaly detection leverages machine learning algorithms, including Random Forest, Decision Tree, and Bayesian Networks, trained on historical traffic datasets.

The integration of these techniques provides a robust and multi-faceted approach to worm

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

detection, offering improved accuracy, real-time responsiveness, and adaptability to emerging cyber threats. By combining signature-based and anomaly-based detection, you get a broader coverage. Signature-based detection can catch known worms, while anomaly-based detection can pick up on new, unidentified threats that don't match any known signatures.

Anomaly detection is particularly useful for identifying new or evolving worms that may not have established signatures yet. This early detection can help mitigate potential damage before a worm spreads widely.

While signature-based detection is precise, it can sometimes generate false positives.

Advantages Of Proposed System

By combining signature-based and anomaly-based detection, you get a broader coverage. Signature-based detection can catch known worms, while anomaly-based detection can pick up on new, unidentified threats that don't match any known signatures.

Anomaly detection is particularly useful for identifying new or evolving worms that may not have established signatures yet. This early detection can help mitigate potential damage before a worm spreads widely.

While signature-based detection is precise, it can sometimes generate false positives.

VI. IMPLEMETATION

The implementation of the Two-Factor Worm Detection system involves integrating signature-based and anomaly-based detection techniques to enhance threat identification and mitigation. The system architecture comprises data collection, preprocessing, feature extraction, model training, and real-time detection components.

1. **Data Collection and Preprocessing:**

Capture network traffic using PCAP datasets. Extract network flow features such as source IP, destination IP, port numbers, protocol type, packet size, and connection duration. Normalize and clean the dataset to remove inconsistencies and redundant data.

2. **Signature-Based Detection Implementation:**

Utilize known worm signatures stored in a database. Compare incoming network traffic against stored signatures. If a match is found, classify the traffic as a known worm and trigger an alert.

3. **Anomaly-Based Detection Implementation:**

Train machine learning models using historical traffic datasets. Utilize Random Forest, Decision Tree, and Bayesian Networks for classification. Define normal traffic patterns and detect

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

deviations. If an anomaly is detected, further analyze the behavior to confirm worm activity.

4. **Algorithmic Implementation: Signature-Based Detection Algorithm:**

Input: Captured network traffic packet. Extract relevant traffic features. Compare extracted features against the known signature database .If a match is found, classify as a worm and generate an alert .Else, forward to anomaly detection.

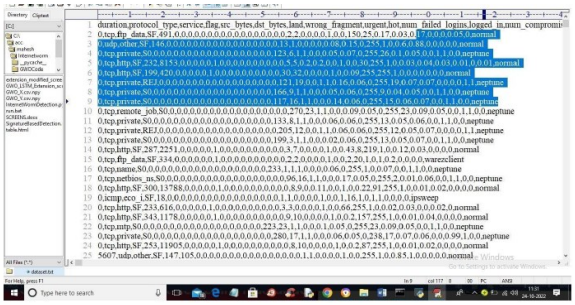
5 Anomaly-Based Detection Algorithm:

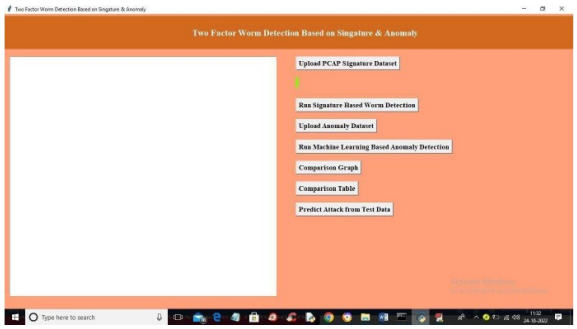
Input: Network traffic dataset. Preprocess and extract relevant features. Train machine learning models (Random Forest, Decision Tree, Bayesian Networks) on labeled data. During detection, classify incoming traffic as normal or anomalous. If classified as anomalous, generate an alert for potential worm activity.

6.Real-time Detection and Response:

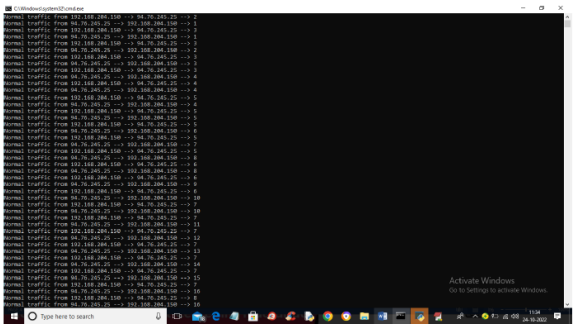
Continuously monitor network traffic for potential worm threats. If a worm is detected, trigger an automated response to block malicious traffic. Update anomaly detection models periodically with new traffic data. The combined approach ensures comprehensive worm detection by leveraging the strengths of both signature-based precision and anomaly-based adaptability, leading to improved real-time responsiveness and mitigation of emerging threats.

VII RESULTS

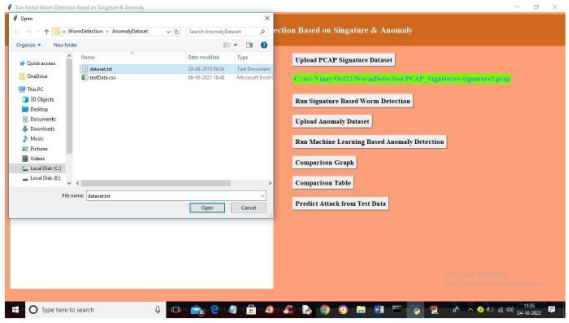


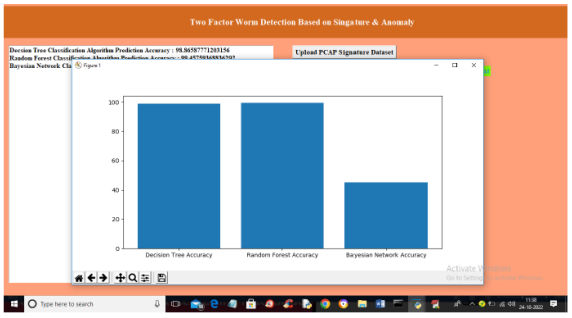


DATASETS OF SIGNATURE & ANOMALY



UPLOAD ANOMALY DATASET





ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

VIII CONCLUSION

With cyber threats evolving rapidly, securing networks has never been more important. Our research introduces a two-way factor authentication system that combines signature-based and anomaly-based detection techniques to enhance security. The signature-based method quickly detects known threats by comparing network traffic to existing worm signatures. However, since new threats constantly emerge, we integrate anomaly-based detection powered by machine learning models like Random Forest, Decision Trees, and Bayesian Networks. By analyzing network traffic, monitoring unusual activity, and using honeypots to lure attackers, our system identifies both known and unknown threats before they cause damage.

A key strength of our approach is its adaptability. The use of honeypots helps track malicious activity, while continuous machine learning updates improve accuracy over time. By blending traditional detection with AI-driven techniques, we achieve better threat identification while minimizing false alarms.

FUTURE SCOPE

To further enhance security, we aim to: Improve real-time detection efficiency. Refine models with deep learning for better accuracy. Integrate AI-driven threat intelligence for proactive defense. Expand detection beyond worms to broader cyber threats .By continuously evolving, our approach helps build safer, more resilient digital networks.

REFERENCES

1. Guoxin Security Research Institute. 2016-2017 Global Cyberspace Security Roundup [z]. 2017,11,17.
2. Kaur R, Singh M. A Survey on Zero-Day Polymorphic Worm Detection Techniques[J]. IEEE Communications Surveys & Tutorials, 2014, 16(3):1520-1549.
3. Aljawarneh S A, Moftah R A, Maatuk A M. Investigations of automatic methods for detecting the polymorphic worms signatures[J]. Future Generation Computer Systems, 2016, 60:67-77.
4. Bayoğlu B, İbrahim Soğukpınar. Graph based signature classes for detecting polymorphic worms via content analysis[J]. Computer Networks, 2012, 56(2):832-844.
5. Tang Y, Xiao B, Lu X. Signature tree generation for polymorphic worms[J]. IEEE transactions on computers, 2011, 60(4): 565-579.
6. Automated signature generation for polymorphic worms using Substrings extraction and Principal Component Analysis
7. Automatic signature generation for polymorphic worms by combination of token extraction and sequence alignment approaches | IEEE Conference Publication | IEEE Xplore
8. Two Factor Worm Detection on Signature and Anomaly - IJFMR
9. 25_online_apr_CMRIT.pdf
10. www.youtube.com