International Journal of Advanced Multidisciplinary Research and Educational Development
Volume 2, Issue 2 | March – April 2026 | www.ijamred.com
ISSN: **3107-6513**

Zero-Day Malware Behaviour Monitoring System

K.Joy Abishaya , Ms.V.Yogashri

Department of Computer Science, Rathinam College of Arts and Science (Autonomous), Coimbatore, Tamilnadu, India.

Abstract *- Zero-day malware has become a critical cybersecurity threat, exploiting unknown vulnerabilities to infiltrate systems without prior detection. These attacks are highly dangerous because traditional signature-based security systems fail to recognize new and unseen malware variants. Early detection is essential to safeguard sensitive data, ensure system integrity, and maintain secure computing environments, but conventional methods often struggle to identify evolving and sophisticated malicious behaviors.This project proposes an intelligent Zero-Day Malware Behaviour Monitoring System that focuses on detecting suspicious activities rather than relying solely on known malware signatures. The system continuously monitors system behavior such as file access patterns, process execution, memory usage, and network activity. By analyzing these behavioral patterns, it identifies anomalies that may indicate the presence of zero-day malware.The system utilizes machine learning techniques combined with behavior-based analysis to improve detection accuracy. It extracts features from real-time system activities and classifies them as normal or malicious using trained models. Compared to traditional approaches, this method offers higher adaptability, faster detection, and improved capability to handle unknown threats.*

Keywords *– Zero-Day Malware, Behaviour Monitoring System, Anomaly Detection, Machine Learning, Cybersecurity, Feature Extraction, Real-Time Monitoring, Malicious Activity Detection, System Behaviour Analysis, Network Activity Monitoring.*

1. Introduction

The rapid growth of digital technology and internet usage has significantly increased the risk of cyber threats, among which zero-day malware attacks are considered one of the most dangerous. Zero-day malware refers to newly emerging malicious software that exploits unknown vulnerabilities in a system, making it difficult for traditional security solutions to detect and prevent such attacks. Since these threats do not have predefined signatures, conventional antivirus and rule-based detection systems often fail to identify them in time.

To overcome these limitations, there is a need for an advanced and intelligent approach that focuses on monitoring system behavior rather than relying solely on known threat patterns. The Zero-Day Malware Behaviour Monitoring System is designed to detect suspicious activities by continuously analyzing system operations such as file access, process execution, memory usage, and network communication. By identifying unusual or abnormal patterns, the system can effectively detect potential threats at an early stage.

This project incorporates machine learning techniques to improve detection accuracy and adaptability. By extracting relevant features from system activities and training models to distinguish between normal and malicious behavior, the system becomes capable of identifying previously unseen malware. This behavior-based approach enhances the system's ability to respond to evolving cyber threats.

Overall, the proposed system provides a reliable, scalable, and efficient solution for real-time detection of zero-day malware. It plays a crucial role in strengthening cybersecurity by protecting systems and sensitive data from advanced and unknown attacks.

The increasing use of computers and the internet has led to a rise in cyber threats, especially zero-day malware attacks, which exploit unknown vulnerabilities and cannot be detected by traditional

ISSN: 3107-6513

security systems. These attacks are highly dangerous because they do not have predefined signatures, making conventional antivirus methods ineffective. To address this issue, the Zero-Day Malware Behaviour Monitoring System focuses on detecting malicious activities by continuously monitoring system behavior such as file access, process execution, memory usage, and network activity. By analyzing these behaviors and identifying unusual patterns, the system can detect potential threats in real time. This project uses machine learning techniques to extract important features and classify activities as normal or malicious, improving detection accuracy and adaptability. Therefore, the proposed system provides an efficient and reliable solution for identifying unknown malware and enhancing overall cybersecurity.

.

2.Related Works

Several research studies have been conducted to address the challenges of detecting zero-day malware using advanced techniques. Traditional signature-based detection methods have been widely used, but they are ineffective against new and unknown threats. To overcome this limitation, researchers have focused on behavior-based analysis, where system activities such as file operations, memory usage, and network traffic are monitored to identify suspicious patterns. Many studies have applied machine learning algorithms like Decision Trees, Support Vector Machines, and Neural Networks to classify malicious and normal behavior based on extracted features. Additionally, some approaches use anomaly detection techniques to identify deviations from normal system behavior, which helps in detecting previously unseen malware. Recent works also integrate real-time monitoring systems with automated alert mechanisms to improve response time and system security. These advancements highlight the importance of intelligent, adaptive, and scalable solutions for effective zero-day malware detection.

In recent years, machine learning-based approaches have gained popularity in zero-day malware detection. Researchers have used supervised learning algorithms such as Support Vector Machines (SVM), Random Forest, and Naive Bayes to classify system activities as benign or malicious. These models are trained using large datasets containing features like system calls, file behavior, and network traffic patterns. The use of machine learning helps in improving detection accuracy and reduces false positives.

o

3.System Design

The background research indicates a growing need for intelligent systems in detecting phishing websites using network-based techniques. This study introduces an optimized approach for identifying phishing websites by analyzing URL characteristics and network-level information to achieve higher detection accuracy. The schematic representation of the proposed system is illustrated.The primary contributions of this study are outlined as follows:

(i)Implementing effective URL preprocessing techniques to ensure accurate and clean input data for analysis.
(ii)Utilizing feature extraction methods to identify significant URL and network features that indicate phishing behavior.
(iii)Rule-based detection techniques is to classify websites as legitimate or phishing based on analyzed data.
(iv) Analyzing network-related attributes such as DNS records, IP address behavior, and traffic patterns to detect suspicious activities.

3.1 URL Input & Preprocessing

This process begins with the user entering a website URL into the system. The system validates the input to ensure it is correctly formatted and usable. Any unnecessary characters or errors are removed during preprocessing. The cleaned and standardized URL is then passed to the next stage for further analysis.

3.2. Feature Extraction

In this process, important features are extracted from the given URL. These include lexical features such as URL length and special characters, as well as structural features like domain information. The extraction helps in identifying patterns that may indicate phishing. The processed feature set is then forwarded for deeper analysis.

3.3. Network Analysis

This process focuses on analyzing network-related information of the website. It examines DNS records, IP address details, and server behavior to detect suspicious activity. Traffic patterns and response characteristics are also

ISSN: 3107-6513

considered. The analyzed network data plays a key role in identifying potential phishing threats.

3.4. Technique Selection

The research focuses on analyzing URL characteristics and network-related data for phishing website detection. To identify the most suitable approach, various network-based techniques were studied and selected based on their effectiveness in detecting suspicious activities. These techniques are widely used in cybersecurity for identifying malicious websites through communication and domain analysis. The selected techniques include:

- DNS Analysis
- IP Address Verification
- URL Inspection

Considering the nature of the dataset and the objective of detecting phishing websites, these techniques were chosen for their ability to identify abnormal patterns and improve detection accuracy.

3.4.1. DNS Analysis

DNS (Domain Name System) Analysis is an important technique used to examine domain-related information of a website. It helps in identifying suspicious domains by analyzing factors such as domain age, registration details, and DNS record consistency. Phishing websites often use newly registered domains or frequently change their DNS records to avoid detection. This technique also checks mismatches between domain names and their associated records. By monitoring DNS behavior, abnormal patterns can be detected effectively. DNS analysis plays a key role in identifying hidden malicious activities. It improves the reliability of phishing detection systems.

3.4.2. IP Address Verification

IP Address Verification focuses on analyzing the IP address associated with a website. It helps in determining whether the IP address is trustworthy or linked to malicious activities. Phishing websites often use suspicious, shared, or dynamically changing IP addresses. This technique checks if the IP address is blacklisted or associated with multiple domains. It also verifies consistency between the domain name and its IP location. Any mismatch or unusual pattern may indicate a phishing attempt. This method enhances detection accuracy by validating network-level information.

3.4.3. URL Inspection

URL Inspection is used to analyze the structure and components of a website URL. It examines features such as URL length, use of special characters, presence of misleading words, and abnormal patterns. Phishing URLs often mimic legitimate websites but include slight variations that are difficult to notice. This technique also checks for multiple redirections and suspicious domain names. By identifying irregular patterns, the system can detect malicious intent. URL inspection is simple yet highly effective in phishing detection. It acts as a primary step in identifying suspicious websites.

3.4.4. System Evaluation

System evaluation is carried out to measure the performance of the phishing detection system. Various metrics such as accuracy, precision, recall, and F1 score are used for evaluation. These metrics help in understanding how well the system identifies phishing websites and avoids false detections. A good system should have high accuracy and low false positive rates. Evaluation is performed using both known and unseen data to ensure reliability. This process helps in improving the system's effectiveness. It ensures that the system performs efficiently in real-time scenarios.

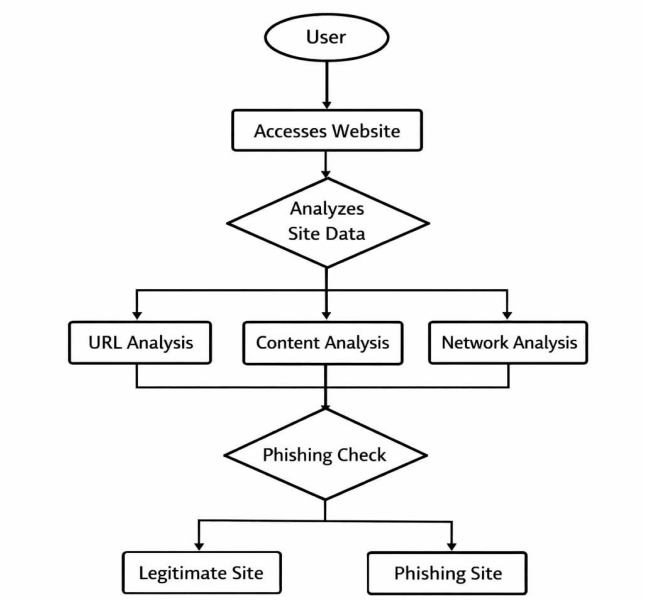

Fig 1. Dataflow Diagram

4. Object and Scope

The objective of this research is to develop an intelligent system for detecting phishing websites using network-based techniques. The primary goal is to accurately identify malicious URLs by analyzing their features and network-related patterns, thereby protecting users from cyber threats and data breaches. This study aims to improve detection accuracy, reduce false positives, and enhance the system's ability to identify newly emerging phishing attacks. By

ISSN: 3107-6513

utilizing advanced analysis of network behavior and URL characteristics, the research seeks to provide a reliable and efficient solution for real-time phishing detection. The scope of this research includes a detailed analysis of various characteristics of web URLs, such as lexical, structural, and statistical features, along with network-level attributes to distinguish between legitimate and phishing websites. The study focuses on designing and evaluating an intelligent detection system using collected datasets and comparing its performance in terms of accuracy and efficiency.

5.Literature Review

Phishing website detection has gained significant attention in recent years due to the rapid increase in cyber threats and the growing dependence on online platforms. The rise of sophisticated phishing attacks, which exploit deceptive URLs and closely mimic legitimate websites, has created a strong need for more advanced and intelligent detection systems. Traditional security methods based on fixed rules and blacklists are no longer sufficient to handle evolving attack strategies, especially with the emergence of zero-day phishing attacks. As a result, recent research has increasingly focused on network-based techniques and intelligent analysis methods to improve the accuracy and efficiency of phishing detection systems.

A review of recent studies highlights the effectiveness of network-based approaches in detecting phishing websites by analyzing communication patterns and domain-related information. Techniques such as DNS analysis, IP address verification, traffic monitoring, and server response evaluation are widely used to identify suspicious behavior associated with phishing activities. These approaches analyze features such as URL structure, domain characteristics, packet flow, and redirection patterns to distinguish between legitimate and malicious websites. Compared to traditional methods, network-based detection systems provide better adaptability and real-time monitoring capabilities. Overall, these techniques enhance detection performance, improve reliability, and play a crucial role in strengthening cybersecurity against modern phishing attacks.

6. Output

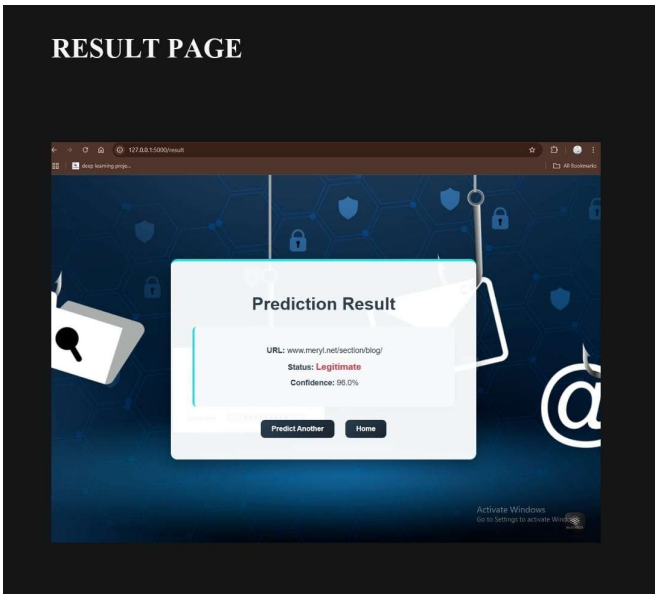

Fig 2.Result Page

7. Results

The results obtained from the proposed system are presented in a structured format to evaluate its effectiveness in detecting phishing websites. The performance is analyzed based on key metrics such as accuracy, precision, recall, and F1 score. The results are organized to highlight the efficiency of different network-based techniques used in the system. This arrangement enables easy comparison and helps in identifying the most effective techniques for phishing detection. It also provides a clear understanding of the system's strengths and its ability to handle real-time cyber threats.

Recent studies have emphasized the importance of network-based approaches in improving phishing detection systems. Researchers have proposed various techniques that analyze domain information, IP address behavior, and traffic patterns to identify malicious websites. These approaches focus on detecting abnormal network activities and inconsistencies in domain records. By integrating multiple network-level features, the detection system becomes more reliable and efficient.

8.Conclusion

The proposed system for phishing website detection using network-based techniques provides effective and reliable results in identifying malicious websites. By analyzing URL characteristics along with network-related features such as DNS records, IP address behavior, and traffic patterns, the system is able to accurately distinguish between legitimate

ISSN: **3107-6513**

and phishing websites. Among the techniques used, network analysis proved to be highly effective in detecting suspicious activities and improving overall detection performance. The system demonstrated strong accuracy and consistency when evaluated using different datasets.

By incorporating factors such as domain information, URL structure, and real-time network behavior, the system can identify complex phishing patterns and prevent potential cyber threats. This enables better decision-making in securing online platforms and protecting user data. Although challenges such as dynamic phishing techniques and evolving attack patterns exist, continuous improvements in network monitoring and analysis methods can further enhance system performance. Overall, the proposed approach provides a scalable and efficient solution for real-time phishing detection and contributes to strengthening modern cybersecurity systems.

9. References

[1] Abu-Nimeh, S., Nappa, D., Wang, X., and Nair, S., "A comparison of phishing detection techniques," *Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit*, 2007, pp. 6–69.

[2] Zhang, Y., Hong, J.I., and Cranor, L.F., "CANTINA: A content-based approach to detecting phishing websites," *Proceedings of the 16th International World Wide Web Conference*, 2007, pp. 639–648.

[3] Garera, S., Provos, N., Chew, M., and Rubin, A.D., "A framework for detection and measurement of phishing attacks," *Proceedings of the 2007 ACM Workshop on Recurring Malcode*, pp. 1–8.

[4] Ma, J., Saul, L.K., Savage, S., and Voelker, G.M., "Beyond blacklists: Learning to detect malicious web sites from suspicious URLs," *Proceedings of the 15th ACM SIGKDD International Conference*, 2009, pp. 1245–1254.

[5] Xiang, G., Hong, J., Rose, C.P., and Cranor, L., "CANTINA+: A feature-rich machine learning framework for detecting phishing web sites," *ACM Transactions on Information and System Security*, 2011.

[6] Le, A., Markopoulou, A., and Faloutsos, M., "PhishDef: URL names say it all," *IEEE INFOCOM*, 2011, pp. 191–195.

[7] Verma, R. and Das, A., "What's in a URL: Fast feature extraction and malicious URL detection," *Proceedings of the 3rd ACM Workshop on Security and Artificial Intelligence*, 2010.

[8] Thomas, K., Grier, C., Ma, J., Paxson, V., and Song, D., "Design and evaluation of a real-time URL spam filtering service," *IEEE Symposium on Security and Privacy*, 2011.

[9] Sahoo, D., Liu, C., and Hoi, S.C.H., "Malicious URL detection using machine learning: A survey," *ACM Computing Surveys*, 2017.

[10] Almomani, A., Gupta, B.B., Atawneh, S., Meulenberg, A., and Almomani, E., "A survey of phishing email filtering techniques," *IEEE Communications Surveys & Tutorials*, 2013.

[11] Mohammad, R.M., Thabtah, F., and McCluskey, L., "Phishing detection: A recent intelligent machine learning comparison based on models content and features," 2014 IEEE International Conference on Intelligence and Security Informatics, pp. 72–77.

[12] Basnet, R.B., Mukkamala, S., and Sung, A.H., "Detection of phishing attacks: A machine learning approach," Studies in Fuzziness and Soft Computing, Springer, 2008, pp. 373–383.

[13] Bergholz, A., De Beer, J., Glahn, S., Moens, M.F., Paaß, G., and Strobel, S., "New filtering approaches for phishing email," Journal of Computer Security, vol. 18, no. 1, 2010, pp. 7–35.

ISSN: **3107-6513**

[14] Khonji, M., Iraqi, Y., and Jones, A., "Phishing detection: A literature survey," IEEE Communications Surveys & Tutorials, vol. 15, no. 4, 2013, pp. 2091–2121.

[15] Jain, A.K. and Gupta, B.B., "Phishing detection: Analysis of visual similarity-based approaches," Security and Communication Networks, vol. 7, no. 5, 2014, pp. 863–875.

10. Acknowledgment

This article is the outcome of the research work carried out in the **Department of Computer Science.** The authors would like to express their sincere gratitude to the Department for providing the necessary support and resources to successfully complete this work. We also extend our thanks to the faculty members and mentors for their valuable guidance and encouragement throughout the research. Their continuous support has greatly contributed to the successful development of this project.