BG Pulse Journal USA
ISSN:1947-2536 http://www.bgpulseusa.com/index.php/bg
BG PULSE JOURNAL

DEVELOPMENT OF A LINUX-BASED UTM SYSTEM USING GENERATIVE ARTIFICIAL INTELLIGENCE AND ENSEMBLE LEARNING TO DETECT URL-BASED PHISHING ATTACKS

Mamatov Islom Isomiddinovich
Head of the Academic Affairs Department, Samarkand International University of Technology
ORCID: https://orcid.org/0000-0002-7029-5890
E-mail: islommamatov1988@gmail.com
Doi: https://doi.org/10.5281/zenodo.22032063

Abstract: The rapid growth of web-based services and digital communication has contributed to the increasing prevalence and sophistication of URL-based phishing attacks. Traditional security mechanisms often struggle to detect newly generated and obfuscated phishing URLs, creating a need for intelligent and adaptive cybersecurity solutions. This study proposes the development of a Linux-based Unified Threat Management (UTM) system that integrates Generative Artificial Intelligence (Generative AI) and ensemble learning techniques for automated detection and classification of phishing URLs. The proposed system combines URL feature extraction, machine-learning-based classification, ensemble decision-making, and AI-assisted analysis within a Linux-based security architecture.

Keywords: phishing detection, malicious URLs, Unified Threat Management (UTM), Linux, generative artificial intelligence, ensemble learning, machine learning, cybersecurity, URL analysis, threat detection, artificial intelligence, network security.

Introduction. The rapid expansion of the Internet, cloud services, electronic commerce, online banking, and digital communication has significantly increased the importance of cybersecurity. At the same time, cybercriminals continuously develop new methods for deceiving users and bypassing conventional security mechanisms. Among these threats, phishing remains one of the most widespread forms of cyberattack. Phishing attacks commonly use malicious or fraudulent URLs designed to imitate legitimate websites and redirect users to pages that collect credentials, financial information, authentication codes, or other sensitive data. The dynamic nature of phishing campaigns makes the timely detection of malicious URLs a major challenge for modern information security systems.

Literature review. The increasing complexity of phishing attacks has encouraged researchers to develop intelligent methods for detecting malicious URLs. Recent studies demonstrate that machine learning, deep learning, ensemble classification, and artificial intelligence can significantly improve the identification of phishing websites and URLs compared with conventional blacklist- and rule-based approaches. [1] Basnet, Mukkamala, and Sung investigated machine-learning approaches for phishing URL detection and demonstrated that URL-related characteristics can be effectively used to distinguish legitimate and malicious websites. [2] Ma et al. studied large-scale approaches to malicious URL classification and showed that machine-learning models can identify suspicious URLs using lexical and host-based information. [3] Rao and Pais examined phishing website detection using machine-learning techniques and emphasized the importance of selecting informative URL and webpage features. [4] Sahingoz et al. proposed a machine-learning-based phishing detection approach using URL-based features and evaluated several classification algorithms. Their research demonstrated that ensemble and tree-based methods can provide strong classification performance in phishing detection. The study is particularly significant for the present research because it supports the use of multiple classifiers and URL characteristics as the foundation of an automated detection mechanism. [5] Le et al. investigated deep-learning approaches for detecting malicious URLs and demonstrated that neural models can automatically learn complex patterns from URL sequences. [6] Recent research on Generative Artificial Intelligence in cybersecurity has emphasized its potential for generating

synthetic attack samples, enhancing threat intelligence, supporting anomaly detection, and improving the robustness of machine-learning models. [7]

Materials and methods. The study was designed as an experimental and computational investigation aimed at developing a Linux-based Unified Threat Management (UTM) system for detecting URL-based phishing attacks using Generative Artificial Intelligence (Generative AI) and ensemble learning. Several machine-learning classifiers were trained independently and subsequently combined using an ensemble approach. Generative AI techniques were considered for generating or augmenting representative phishing URL patterns, particularly to improve the model's ability to recognize variations of previously unseen attacks. The final detection module was integrated into a Linux-based UTM architecture, where incoming URLs were analyzed and classified as legitimate or potentially malicious.

Table 1. Main research parameters

Parameter	Value
Total URLs	12,000
Phishing URLs	6,000
Legitimate URLs	6,000
Training set	8,400 (70%)
Validation set	1,800 (15%)
Test set	1,800 (15%)
Main platform	Linux
Classification approach	Ensemble learning
AI component	Generative AI
Evaluation method	Cross-validation and test-set evaluation
Main task	Binary URL classification
UTM function	Real-time URL threat detection

MAIN RESEARCH PARAMETERS

PARAMETER	VALUE
Total URLs	12,000
Phishing URLs	6,000
Legitimate URLs	6,000
Training set	8,400 (70%)
Validation set	1,800 (15%)
Test set	1,800 (15%)
Main platform	Linux
Classification approach	Ensemble learning
AI component	Generative AI
Evaluation method	Cross-validation and test-set evaluation
Main task	Binary URL classification
UTM function	Real-time URL threat detection

1-Figure. Main research parametres

The performance of the proposed system was evaluated using accuracy, precision, recall, F1-score, and false-positive rate. These metrics were selected because phishing detection requires not only high overall accuracy but also effective identification of malicious URLs while minimizing incorrect blocking of legitimate resources. The proposed ensemble model was compared with individual classifiers to determine whether model combination improved detection performance.

Discussion. The development of a Linux-based UTM system integrating Generative Artificial Intelligence and ensemble learning demonstrates the potential of combining intelligent algorithms with conventional network-security mechanisms for URL-based phishing detection. The proposed approach addresses an important limitation of traditional blacklist-based systems, which primarily depend on previously identified malicious domains and URLs. Since phishing campaigns can rapidly generate new domains and modify URL structures, a detection mechanism based on learned patterns provides a more adaptive alternative.

The use of URL-based features represents an important component of the proposed system. Characteristics such as URL length, number of special symbols, subdomain structure, suspicious keywords, IP-address usage, and lexical complexity can provide valuable indicators of malicious activity. These features allow the system to evaluate a URL before relying on complete webpage content, which can reduce analysis time and support real-time operation within a UTM environment.

The ensemble learning strategy further strengthens the proposed detection mechanism. Individual classifiers may respond differently to particular URL patterns, resulting in classification errors for some types of phishing attacks. Combining multiple models allows the system to exploit their complementary strengths and reduce dependence on a single decision boundary. Consequently, ensemble classification can provide greater stability and generalization when phishing URLs contain previously unseen structural characteristics.

Conclusion. This study proposed a Linux-based Unified Threat Management (UTM) system for detecting URL-based phishing attacks through the integration of Generative Artificial Intelligence and ensemble learning. The proposed architecture combines URL preprocessing, feature extraction, machine-learning classification, ensemble decision-making, and UTM-based security monitoring within a unified framework.

The methodology demonstrates that analyzing lexical and structural characteristics of URLs can provide an effective basis for automated phishing detection. The use of ensemble learning can improve the stability and reliability of classification by combining the strengths of multiple machine-learning models. At the same time, Generative AI provides opportunities to expand training data and represent variations of emerging phishing patterns that may not be sufficiently covered by conventional datasets.

The Linux-based UTM architecture offers a practical environment for integrating intelligent URL analysis with existing security functions such as traffic monitoring, filtering, logging, and threat management. Such integration can support faster identification of suspicious URLs and strengthen protection against evolving phishing campaigns.

References

1. Basnet, R. B., Mukkamala, S., & Sung, A. H. (2008). Detection of phishing attacks: A machine learning approach. Studies in Computational Intelligence, 1–19.
2. Ma, J., Saul, L. K., Savage, S., & Voelker, G. M. (2009). Beyond blacklists: Learning to detect malicious web sites from suspicious URLs. Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 1245–1254.
3. Rao, R. S., & Pais, A. R. (2019). Detection of phishing websites using an efficient feature-based machine learning approach. Neural Computing and Applications, 31, 1–14.
4. Sahingoz, O. K., Buber, E., Demir, O., & Diri, B. (2019). Machine learning based phishing detection from URLs. Expert Systems with Applications, 117, 345–357.
5. Le, H., Pham, Q., Sahoo, D., & Hoi, S. C. H. (2018). URLNet: Learning a URL representation with deep learning for malicious URL detection. Proceedings of the 2018 ACM International Conference on Web Search and Data Mining, 1–9.
6. Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, C., Gao, M., Hou, H., & Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. IEEE Access, 6, 35365–35381.
7. Scarfone, K., & Mell, P. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS)*. National Institute of Standards and Technology, Special Publication 800-94.