International Journal of Web of Multidisciplinary Studies
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
website: https://ijwos.com
Volume 3 Issue 4 , April 2026
OPEN ACCESS
E-ISSN : 3049-2424
DOI: https://doi.org/10.71366/ijwos03042603819

LITERATURE SURVEY ON CYBER SECURITY FOR IDENTIFICATION OF URL BASED ATTACKS USING IP DATA

MADAMANCHI HARSHAVARDHAN[1], PADARTHI MANISH[2], PEDIPINA MAHESH[3], VINJAM NAVEEN[4], VINUKONDA VEERENDRA[5], MRS.SAHANA[6], MRS.SWEETY JULIA[7]

[1,2,3,4,5] 4th year CSE(CYBER SECURITY) Department, JNN Institute Of Enginnering, Chennai.
[6] Assistant Professor of CSE(CYBER SECURITY) Department, JNN Institute Of Enginnering, Chennai.
[7] HOD of CSE(CYBER SECURITY) Department, JNN Institute Of Enginnering, Chennai..

Article Info

Article History:

Published:7 April 2026

Publication Issue:
Volume 3, Issue 4
April-2026

Page Number:
55-57

Corresponding Author:
PEDIPINA MAHESH

Abstract:

With the rapid growth of internet usage, cyber threats such as phishing, malware distribution, and malicious URL attacks have significantly increased. Identifying harmful URLs in real time is crucial to ensure user safety and protect sensitive information. This project focuses on the detection of URL-based attacks using IP data by analyzing various characteristics associated with URLs and their corresponding IP addresses. The proposed system utilizes machine learning techniques to classify URLs as either legitimate or malicious based on features such as IP address patterns, domain information, URL length, presence of special characters, and hosting details. By extracting and analyzing these features, the system can effectively identify suspicious activities and potential threats.

Keywords: cyber threats

1. INTRODUCTION

In today's digital era, the internet plays a vital role in communication, business, education, and daily activities. However, this rapid growth has also led to an increase in cyber threats, especially URL-based attacks such as phishing, malware distribution, and malicious website redirection. Attackers often use deceptive URLs and suspicious IP addresses to trick users into revealing sensitive information or downloading harmful content.

Traditional security systems rely heavily on blacklists and manual monitoring, which are often inefficient in detecting newly generated or unknown malicious URLs. As cyber attackers continuously evolve their techniques, there is a need for a more intelligent and automated approach to identify threats in real time.

2. OBJECTIVES OF THE SURVEY

This survey is carried out with the following goals:

- To study different types of URL-based attacks
- To examine the role of IP data in attack detection
- To analyze existing detection techniques

- To identify key features used in URL classification

3. REVIEW OF EXISTING WORK

3.1 BLACKLISTING TECHNIQUES

Early detection systems relied on maintaining databases of known malicious URLs. These blacklists are used by browsers and security tools to block access to harmful websites. While effective for previously identified threats, this approach fails to detect newly created or unknown (zero-day) malicious URLs.

3.2 HEURISTIC BASED DETECTION

Heuristic methods analyze predefined rules such as URL length, use of special characters, abnormal domain names, and suspicious IP patterns. These techniques are faster than blacklist methods but may produce false positives and are less effective against sophisticated attacks.

3.3 MACHINE LEARNING APPROACHES

Recent studies have applied machine learning algorithms to classify URLs as benign or malicious. Algorithms such as Decision Tree, Random Forest, Naïve Bayes, and Support Vector Machine have been widely used. These models are trained on features like URL structure, domain information, and IP-related data, improving detection accuracy and adaptability.

3.4 DEEP LEARNING TECHNIQUES

Advanced research explores deep learning models such as Neural Networks and LSTM (Long Short-Term Memory) for detecting complex patterns in URLs. These methods can automatically extract features but require large datasets and higher computational resources.

3.5 IP BASED DETYECTION METHODS

Some existing works focus specifically on analyzing IP data, including IP reputation, geolocation, hosting server details, and DNS records. These methods help in identifying suspicious behavior, especially when attackers use direct IP addresses instead of domain names.

4. CONCLUSION

This project presents an effective method for detecting URL-based attacks using IP data and machine learning techniques. By analyzing URL and IP features, the system can accurately identify malicious links, including new and unknown threats. Compared to traditional methods, it offers better accuracy, automation, and real-time detection, improving overall cybersecurity.

References

1. Ma, J., Saul, L. K., Savage, S., & Voelker, G. M. "Beyond Blacklists: Learning to Detect Malicious Web Sites from Suspicious URLs" Proceedings of the ACM SIGKDD, 2009.

2. Garera, S., Provos, N., Chew, M., & Rubin, A. D. "A Framework for Detection and Measurement of Phishing Attacks" ACM Workshop on Recurring Malcode (WORM), 2007.

3. Le, A., Markopoulou, A., & Faloutsos, M. "PhishDef: URL Names Say It All" IEEE INFOCOM, 2011.

4. Sahingoz, O. K., Buber, E., Demir, O., & Diri, B. "Machine Learning Based Phishing Detection from URLs" Expert Systems with Applications, 2019.

5. Sahoo, D., Liu, C., & Hoi, S. C. H. "Malicious URL Detection using Machine Learning: A Survey" ACM Computing Surveys, 2017.