IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026

DOI: 10.17148/IJARCCE.2026.15340

Cybersecurity threat detection to Prevent System

Tikshanaa.P.R[1], Abinaya.Y[2], Dr.R.Nagarajan[3]

Student, BSc Computer Science, Sri Ramakrishna College of Arts & Science, Coimbatore,Tamilnadu,India[1]

Student, BSc Computer Science, Sri Ramakrishna College of Arts & Science, Coimbatore,Tamilnadu,India[2]

Assistant Professor, BSc Computer Science, Sri Ramakrishna College of Arts & Science, Coimbatore,Tamilnadu,India[3]

Abstract Cybersecurity Threat Detection is a system designed to help detect and prevent cyber-attacks in real time. In today's digital world, hackers attempt to steal sensitive data, disrupt services, or damage systems using methods such as malware, phishing, ransomware, and unauthorized access. With the rapid growth of online transactions, cloud computing, and interconnected devices, the risk of cyber threats has increased significantly. This project aims to protect users and organizations by identifying these threats early, generating alerts, and enabling quick defensive action. The system continuously monitors network activity, user behaviour, and system logs to identify anomalies. When a possible threat is detected, it sends an immediate warning and records detailed information for further analysis. Detection techniques include signature-based scanning for known attack patterns, anomaly detection to spot unusual traffic or login attempts, and behavioural analysis to identify suspicious actions from users or devices. By combining these approaches, the system achieves a balance between accuracy and efficiency, reducing false positives while ensuring that genuine threats are not overlooked. The project is developed using HTML, CSS, and JavaScript for the front-end interface, providing a user-friendly dashboard where alerts and logs can be viewed clearly. The Python-based back-end handles data processing, threat detection algorithms, and communication between system components. The dashboard allows administrators to track incidents, analyse patterns, and take corrective measures such as blocking IP addresses, disabling compromised accounts, or applying patches. This system contributes to reducing the risk of cyber-attacks by offering proactive monitoring and timely alerts. It empowers users to safeguard their data, maintain system integrity, and comply with security standards. Beyond individual protection, the project demonstrates how organizations can adopt layered security measures to strengthen resilience against evolving cyber threats. Ultimately, Cybersecurity Threat Detection enhances trust in digital platforms and supports the safe growth of technology-driven environments.

Keywords: Cybersecurity, Threat Detection, Intrusion Detection System (IDS), Anomaly Detection, Malware Prevention, Network Security, Real-Time Monitoring, Incident Response.

I. INTRODUCTION

Cyber-attack is the process of attempting to steal data and gaining unauthorized access to computers and networks using one or more computers. Cyber-attack is usually the initial step taken by cyber criminals to gain unauthorized access to individuals' and businesses' computers and networks before they proceed to commit a data breach. The aim of cyber-attack is usually to disable the targeted computer and shut it down completely or gain access to the data contained within the computer and access connected networks and systems. Cyber-attacks vary greatly in complexity, with cyber criminals launching both random and targeted cyber-attacks against businesses. Various methods are employed by cyber criminals to initiate cyber-attack, and they include denial of service, malware, phishing, and ransomware. The current cyber-attack definition is quite wide-ranging depending on the kind of cyber-attack that cyber criminals have planned to launch. Here are a couple of scenarios illustrating cyber-attack:

Malware: A company does not take the necessary cyber-attack preventive measures and lets employees access any website they want. The employee visits a pretend website, which automatically downloads malware onto the employee's computer. The malware creates a backdoor for a future ransomware cyber-attack.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026

DOI: 10.17148/IJARCCE.2026.15340

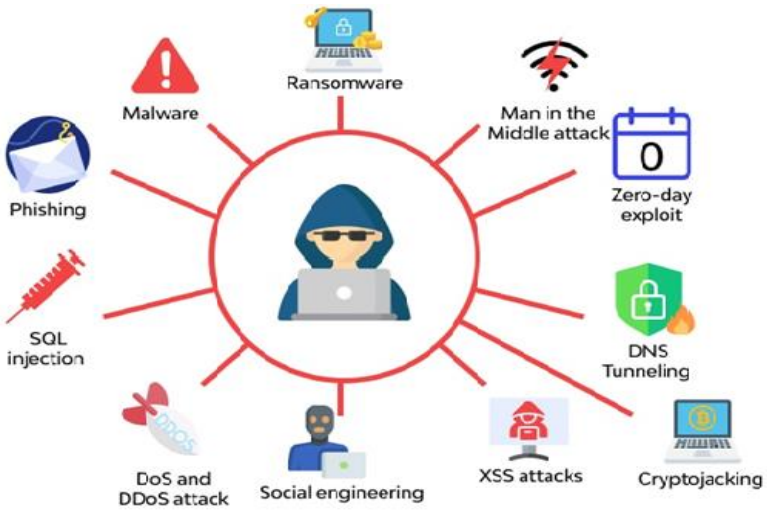

Fig. 1 A sample graph

Overview Diagram

Phishing**:** A phishing email, one of the most common cyber-attack types, gets sent to an employee telling them they need to update their bank account password. They are led to a fake site, and a hacker collects all the information they put in.

II. CONCLUSION

In conclusion, the Cybersecurity Threat Detection system provides an essential layer of protection in today's increasingly digital and interconnected world. By continuously monitoring network activity, user behaviour, and system logs, it can detect and respond to cyber threats in real time, minimizing potential damage and data loss. Its combination of signature-based scanning, anomaly detection, and behavioural analysis ensures accurate threat identification while reducing false positives. The user-friendly dashboard and Python-based back-end empower administrators to track incidents, analyze patterns, and take swift corrective actions. Overall, this system not only strengthens individual and organizational security but also fosters trust in digital platforms, supports compliance with security standards, and enhances resilience against evolving cyber threats, making it a critical tool for safeguarding technology-driven environments.

REFERENCES

[1]. O. Almomani, "A hybrid model using bio-inspired metaheuristic algorithms for network intrusion detection system," *Comput., Mater. Continua,* vol. 68, no. 1, pp. 409–429, 2021, doi: 10.32604/cmc.2021.016113.

[2]. H. Mohammad, T. Alwada'n, O. Almomani, S. Smadi, and N. ElOmari, "Bio-inspired hybrid feature selection model for intrusion detection," *Comput., Mater. Continua*, vol. 73, no. 1, pp. 133–150, 2022, doi: 10.32604/cmc.2022.027475.

[3]. M. A. Almaiah, F. Hajjej, A. Ali, M. F. Pasha, and O. Almomani, "A novel hybrid trustworthy decentralized authentication and data preservation model for digital healthcare IoT based CPS," *Sensors*, vol. 22, no. 4, p. 1448, Feb. 2022, doi: 10.3390/s22041448.

[4]. A. Megantara and T. Ahmad, "A hybrid machine learning method for increasing the performance of network intrusion detection systems," *J. Big Data*, vol. 8, no. 1, pp. 1–19, Dec. 2021, doi: 10.1186/s40537-021-00531-w.

[5]. O. Almomani, "A feature selection model for network intrusion detection system based on PSO, GWO, FFA and GA algorithms," *Symmetry*, vol. 12, no. 6, p. 1046, Jun. 2020, doi: 10.3390/sym12061046.

[6]. X. Huang, J. Liu, Y. Lai, B. Mao, and H. Lyu, "EEFED: Personalized federated learning of execution&evaluation dual network for CPS intrusion detection," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 41–56, 2023, doi: 10.1109/TIFS.2022.3214723.

[7]. R. F. Mansour, "Artificial intelligence based optimization with deep learning model for blockchain enabled intrusion detection in CPS environment," *Sci. Rep.*, vol. 12, no. 1, p. 12937, Jul. 2022, doi: 10.1038/s41598-022-17043-z.

[8]. Alqahtani and S. B. Khan, "An optimal hybrid cascade regional convolutional network for cyberattack detection," *Int. J. Netw. Manage.*, vol. 34, no. 5, p. 2247, Sep. 2024, doi: 10.1002/nem.2247.

[9]. E. C. Nkoro, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, "Detecting cyberthreats in metaverse learning platforms using an explainable DNN," *Internet Things*, vol. 25, Apr. 2024, Art. no. 101046, doi: 10.1016/j.iot.2023.101046.