Samvid Multidisciplinary Research Journ
Where researchers meet their destiny...
ISSN 2582-015X

Cyber Attacks Detection Using Hybrid Models

Mr. Rahulkumar Omprakash Khatri[1], Dr. Mahammad Idrish I. Sandhi[2]

[1] PhD Scholar, Computer Application, Sankalchand Patel University, Visnagar, Gujarat, India
Email: khatrirahul100@gmail.com

[2] Associate Dean, FCS & Head, MCA, SPCE, Sankalchand Patel University, Visnagar, Gujarat, India
Email: idrish.mca@gmail.com

Abstract

The exponential growth of internet-based services, cloud computing, and Internet of Things (IoT) technologies has significantly increased the frequency and sophistication of cyber attacks. Traditional security mechanisms such as firewalls and signature-based intrusion detection systems are no longer sufficient to address modern threats such as zero-day attacks, advanced persistent threats, and polymorphic malware. To overcome these challenges, researchers have proposed hybrid cyber attack detection models that combine multiple techniques including signature-based detection, anomaly detection, machine learning, and deep learning approaches. This review paper presents a comprehensive analysis of hybrid cyber attack detection models, focusing on their architecture, methodologies, datasets, performance metrics, advantages, and limitations. Furthermore, current research challenges and future directions are discussed to provide insights for researchers and practitioners working in the field of cyber security.

Keywords: Cyber Security, Intrusion Detection System, Hybrid Model, Machine Learning, Deep Learning

1. Introduction

Cyber security has become a critical issue in modern computing environments due to the rapid digitalization of services and the increasing dependence on interconnected systems. Organizations across various sectors, including finance, healthcare, education, and government, rely heavily on information systems to store, process, and transmit sensitive data. This dependence has made cyber attacks more attractive and profitable for attackers. Cyber attacks can result in severe consequences such as data breaches, financial losses, service disruptions, and reputational damage.

Traditional cyber security mechanisms primarily rely on static rules or known attack signatures. While these approaches are effective against previously identified threats, they are

incapable of detecting new and evolving attack patterns. Anomaly-based systems attempt to detect deviations from normal behavior, but they often generate high false positive rates. To address these limitations, hybrid cyber attack detection models have been introduced. These models integrate multiple detection techniques to enhance accuracy, adaptability, and robustness against diverse cyber threats.

2. Types of Cyber Attacks

Cyber attacks can be classified into several categories based on their targets and attack mechanisms. Network-based attacks such as Denial of Service (DoS) and Distributed Denial of Service (DDoS) aim to disrupt network availability by overwhelming resources. Application-level attacks, including SQL injection and cross-site scripting, exploit vulnerabilities in software applications. Malware attacks involve malicious software such as viruses, worms, trojans, and ransomware that compromise system integrity and confidentiality. Social engineering attacks manipulate human behavior to obtain sensitive information, while insider attacks originate from authorized users misusing their access privileges.

3. Challenges in Cyber Attack Detection

Detecting cyber attacks in real-world environments presents several challenges. Modern networks generate vast amounts of data, making real-time analysis difficult. Imbalanced datasets, where normal traffic significantly outnumbers attack traffic, affect model performance. Additionally, cyber attacks continuously evolve to evade detection, and zero-day attacks lack prior signatures. High false alarm rates and the need for real-time detection further complicate the deployment of effective security solutions.

4. Traditional Detection Approaches

Signature-based detection identifies attacks by matching patterns against known signatures. Although accurate for known attacks, it fails to detect unknown threats. Anomaly-based detection builds a model of normal behavior and flags deviations as attacks, but it often produces false alarms. Specification-based detection defines legitimate behavior using predefined rules, requiring extensive expert knowledge and maintenance.

5. Machine Learning-Based Detection

Machine learning techniques enable systems to learn from historical data and classify network traffic as normal or malicious. Common algorithms include Decision Trees, Support Vector Machines, K-Nearest Neighbor, Naïve Bayes, and Random Forest. These techniques improve detection accuracy compared to traditional methods but depend heavily on feature selection and labeled datasets.

6. Deep Learning-Based Detection

Deep learning models automatically learn complex features from raw data and have shown superior performance in detecting sophisticated attacks. Models such as Convolutional Neural Networks, Recurrent Neural Networks, Long Short-Term Memory networks, and Autoencoders are widely used in intrusion detection systems. Despite their advantages, deep learning models require large datasets and significant computational resources.

7. Hybrid Cyber Attack Detection Models

Hybrid detection models combine multiple detection techniques to leverage their individual strengths. A typical hybrid system integrates signature-based detection for known attacks and anomaly-based or learning-based methods for unknown threats. Hybrid models may also combine machine learning and deep learning algorithms or incorporate optimization techniques for feature selection.

8. Architecture of Hybrid Detection Systems

A hybrid cyber attack detection system typically consists of data collection, preprocessing, hybrid detection engine, decision-making module, and alert generation components. Data preprocessing includes cleaning, normalization, and feature selection to improve detection performance.

9. Datasets and Performance Metrics

Hybrid detection models are evaluated using benchmark datasets such as KDD Cup 1999, NSL-KDD, UNSW-NB15, CICIDS 2017, and Bot-IoT. Performance metrics include accuracy, precision, recall, F1-score, detection rate, and false positive rate.

10. Advantages and Limitations

Hybrid cyber attack detection models offer improved accuracy, reduced false alarms, and better detection of zero-day attacks. However, they also face limitations such as increased computational complexity, longer training time, and challenges in deployment within resource-constrained environments.

11. Future Research Directions

Future research may focus on lightweight hybrid models for IoT environments, explainable artificial intelligence for transparency, real-time detection systems, and privacy-preserving approaches such as federated learning.

12. Conclusion

Hybrid cyber attack detection models represent a promising solution to modern cyber security challenges. By integrating multiple detection techniques, these models enhance detection accuracy and robustness against diverse attack scenarios. Despite existing challenges,

ongoing advancements in artificial intelligence and computing technologies are expected to further improve the effectiveness and practicality of hybrid detection systems.

References (APA 9th Edition)

Denning, D. E. (1987). An intrusion-detection model. IEEE Transactions on Software Engineering, 13(2), 222–232.
Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems. Military Communications and Information Systems Conference, 1–6.
Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy, 305–316.
Zhang, Y., Chen, X., Guo, D., Song, M., & Teng, Y. (2020). Deep learning-based intrusion detection system for IoT networks. IEEE Access, 8, 123784–123799.