ISSN: 2581-3404 (Online) **IF: 5.445 (SJIF)**

IJIRTM, Volume-7, Issue-3, June-2023.

Cyber Attack Detection in A Network Using Machine Learning

Albert.N.Rejy[1], Dr. Sadhana K. Mishra[2]
M. Tech. Research Scholar[1], Prof. & Head[2]
Dept. of CSE, LNCT, Bhopal[1,2]

Abstract: *Everywhere, cybercrime is on the rise and takes advantage of various computer environment weaknesses. Ethical hackers place more emphasis on identifying vulnerabilities and suggesting methods for mitigating them. In the subject of cyber security, there has been a pressing need for the creation of efficient methods. The majority of IDS approaches now in use are unable to handle the dynamic and intricate nature of cyber attacks on computer networks. Due to machine learning's success in solving problems related to cyber security, it has lately become a topic of significant relevance. For the most difficult problems in cyber security, such as intrusion detection, malware classification and detection, spam detection, and phishing detection, machine learning approaches have been used. Machine learning may identify cyber security risks more effectively than other software-oriented approaches, which lessens the workload on security analysts even if it cannot automate a full cyber security system. As a consequence, effective adaptive approaches, such as various machine learning techniques, can lead to increased detection rates, decreased false alarm rates, and reasonable computation and transmission costs. Our main goal is that the task of finding attacks is fundamentally different from these other applications, making it significantly harder for the intrusion detection community to employmachine learning effectively.*

Keywords: Cyber-crime, Machine learning, Cyber-security, Intrusion detection system.

Introduction

Today, political and commercial entities are increasingly engaging in sophisticated cyber- warfare to damage, disrupt, or censor information content in computer networks. In designing network protocols, there is a need to ensure reliability against intrusions of powerful attackers that can even control a fraction of parties in the network. The controlled parties can launch both passive (e.g., eavesdropping, nonparticipation) and active attacks (e.g., jamming, message dropping, corruption, and forging). Intrusion detection is the process of dynamically monitoring events occurring in a computer system or network, analyzing them for signs of possible incidents and often interdicting the unauthorized access. This is typically accomplished by automatically collecting information from a variety of systems and network sources, and then analyzing the information for possible security problems. Traditional intrusion detection and prevention techniques, like firewalls, access control mechanisms, and encryptions, have several limitations in fully protecting networks and systems from increasingly sophisticated attacks like denial of service. Moreover, most systems built based on such techniques suffer from high false positive and false negative detection rates and the lack of continuously adapting to changing malicious behaviours. In the past decade, however, several Machine Learning (ML) techniques have been applied to the problem of intrusion detection with the hope of improving detection rates and adaptability. These techniques are often used to keep the attack knowledge bases up-to-date and comprehensive. In recent days, cyber-security and protection against numerous cyber-attacks are becoming a burning question. The main reason behind that is the tremendous growth of computer networks and the vast number of relevant applications used by individuals or groups for either personal or commercial use, especially after the acceptance of the Internet of Things (IoT). The cyber-attacks cause severe damage and severe financial losses in large-scale networks. The existing solutions like hardware and software firewalls, user's authentication, and data encryption methods are not sufficient to meet the challenge of upcoming demand, and unfortunately, not able to protect the computer network's several cyber-threats. These conventional security structures are not sufficient as safeguard due to the faster rigorous evolution of intrusion systems. Firewall only controls every access from network to network, which means prevent access between networks. But it does not provide any signal in case of an internal attack. So, it is obvious to develop accurate defense techniques such as machine learning-based intrusion detection system (IDS) for the system's security In general, an intrusion detection system (IDS) is a system or software that detects infectious activities and violations of policy in a network or system. An IDS identifies the inconsistencies and abnormal behavior on a network during the functioning of daily activities in a network or system used to detect risks or attacks related to network security, like denial-of- service (Dos). An intrusion detection system also helps to locate, decide, and control unauthorized system behaviour such as unauthorized access, or modification and destruction. There are different types of intrusion detection systems based on the user perspective. For instance, they are host- based and network-based IDS.

II. Literature Review

An IDS generally has to deal with problems such as large network traffic volumes, highly uneven data distribution, the some research article difficulty to realize decision boundaries between normal and abnormal behavior, and a requirement for continuous adaptation to a constantly changing environment. In general, the challenge is to efficiently capture and classify various behaviours in a computer network. Strategies for classification of network behaviours are typically divided into two categories: misuse detection and anomaly detection. Misuse detection techniques examine both network and system activity for known instances of misuse using signature matching algorithms. This technique is effective at detecting attacks that are already known. However, novel attacks are often missed giving rise to false negatives. Alerts may be generated by the IDS, but reaction to every alert wastes time and resources leading to instability of the system. To overcome this problem, IDS should not start elimination procedure as soon as the first symptom has been detected but rather it should be patient enough to collect alerts and decide based on the correlation of them. Some research statistics with regards to the impact of cybersecurity to businesses, organizations, andindividuals include:

In recent years, cybercrime has been responsible for more than $400 billion in funds stolen and costs to mitigate damages caused by crimes. It has been predicted that a shortage of over 1.8 million cyber security workers will be experienced by 2022. It's been predicted that organizations globally will spend at least $100 billion annually on cyber security protection. Attackers currently make over $1 billion in annual revenue from Ransom ware attacks, such as Wannacry and Crypto Wall attacks.

III. Existing System

Within the ever-growing and quickly increasing field of cyber security, it is nearly impossible to quantify or justify the explanations why cyber security has such an outsized impact. Permitting malicious threats to run any place, at any time or in any context is a long way from being acceptable, and may cause forceful injury. It particularly applies to the Byzantine web of consumers and using the net and company information that cyber security groups are finding it hard to shield and contain. Cyber security may be a necessary thought for people and families alike, also for businesses, governments, and academic establishments that operate inside the compass of the world network or net. With the facility of Machine Learning, we will advance the cyber security landscape. Today's high-tech infrastructure, that has network and cyber security systems, is gathering tremendous amounts of data and analytics on almost all the key aspects of mission-critical systems. Whereas people still give the key operational oversight and intelligent insights into today's infrastructure. Most intrusion detection systems are focused on the perimeter attack surface threats, starting with your firewall. That offers protection of your network's north south traffic, but what it doesn't take into account is the lateral spread (east-west) that many network threats today take advantage of as they infiltrate your organization's network and remain there unseen. We know this is true because research has shown that only 20% of discovered threats come from north south monitoring. When an IDS detects suspicious activity, the violation is typically reported to a security information and event management (SIEM) system where real threats are ultimately determined amid benign traffic abnormalities or other false alarms. However, the longer it takes to distinguish a threat, the more damage can be done. An IDS is immensely helpful for monitoring the network, but their usefulness all depends on what you do with the information that they give you. Because detection tools don't block or resolve potential issues, they are ineffective at adding a layer of security unless you have the right personnel and policy to administer them and act on any threats. An IDS cannot see into encrypted packets, so intruders can use them to slip into the network. An IDS will not register these intrusions until they are deeper into the network, which leaves your systems vulnerable until the intrusion is discovered. This is a huge concern as encryption is becoming more prevalent to keep our data secure. One significant issue with IDS is that they regularly alert you to false positives. In many cases false positives are more frequent than actual threats. An IDS can be tuned to reduce the number of false positives; however, your engineers will still have to spend time responding to them. If they don't take care to monitor the false positives, real attacks can slipthrough or be ignored.

IV. Proposed System

Machine Learning algorithms can be used to train and detect if there has been a cyber attack. As soon as the attack is detected, an email notification can be sent to the security engineers or users. Any classification algorithm can be used to categorize if it is a DoS/DDoS attack or not. One example of a classification algorithm is Support Vector Machine (SVM) which is a supervised learning method that analyses data and recognizes patterns. Since we cannot control when, where or how an attack may come our way, and absolute prevention against these cannot be guaranteed yet, our best shot for now is early detection which will help mitigate the risk of irreparable damage such incidents can cause. Organizations can use existing solutions or build their own to detect cyber attacks at a very early stage to minimize the impact. Any system that requires minimal human intervention would be ideal.

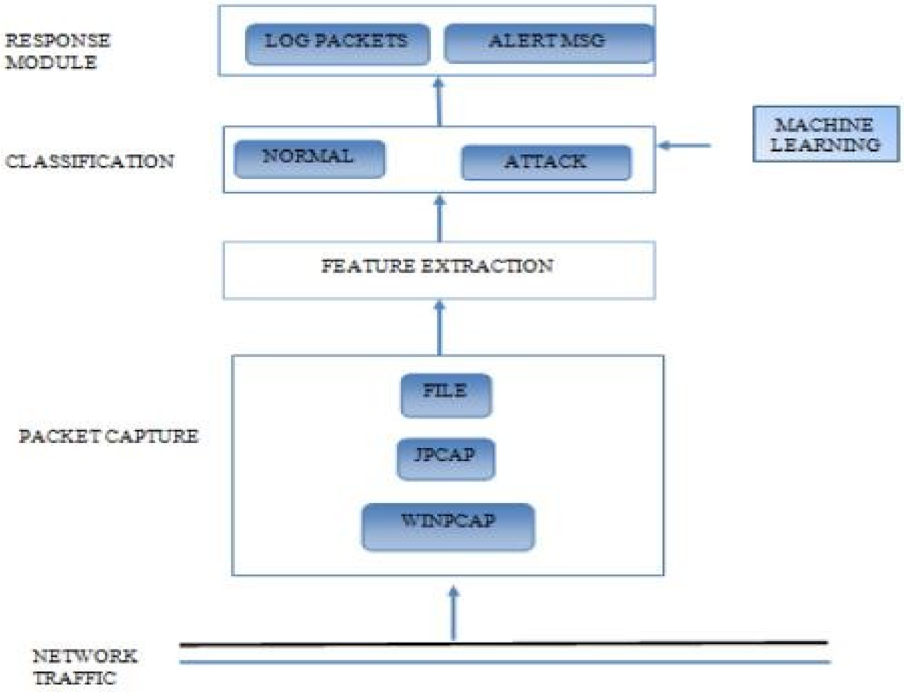

Figure 1: Proposed system architecture.

IMPLEMENTATIONLEVEL:

System level:

Cumulative and per user CPU usage of real and virtual memory Amount of swap space currently available Amount of free memory I/O and disk usage.

1. **User level:**

Type of user and user privileges Login/Logout period and location Access of resources and directories Type of software/programs use Key stroke pattern (use in future) Average number of packets sent and received Duration of theconnection

2. **Process level:**

The number of processes and their types Relationship among processes

3. **Packet level:**

Average number of packets sent and received

V. Conclusion

To locate application layer attacks using artificial intelligence (AI) was suggested in this article. Graph-based division method and dynamic programming are used to obtain examples (in the form of PCRE standard articulations) for the model. In order to show the actual behavior of the apps and to detect digital attacks, the usual articulations are used as a guide. Additionally, we presented the results that show how the suggested computation may effectively be used to locate application layer attacks.

References

[1]. Dipankar Dasgupta. Immunity-based intrusion detection system: A general frame- work. In Proceedings of the 22nd National Information Systems Security Confer-ence (NISSC). Arlington, Virginia, USA, 1999.

[2]. Jonatan Gomez and Dipankar Dasgupta. Evolving fuzzy classi_ers for intrusion detection. In Proceedings of the 2002 IEEE Workshop on Information Assurance,West Point, NY, USA,2002.

[3]. Steven A. Hofmeyr, Stephanie Forrest, and Anil Somayaji. Intrusion detection using sequences of system calls. Journal of Computer Security, 6(3):151{180, August 1998.

[4]. Peter Mell Karen Scarfone. Guide to intrusion detection and prevention systems (idps). National Institute of Standards and Technology, NIST SP - 800-94, 2007.

[5]. Jungwon Kim, Peter J. Bentley, Uwe Aickelin, Julie Greensmith, Gianni Tedesco, and Jamie Twycross. Immune system approaches to intrusion detection { a review. Natural Computing, 6(4):413{466, December 2007.

[6] A. Shabtai, E. Menahem and Y. Elovici. F- Sign: automatic, function-based signature generation for malware, systems, man, and cybernetics, Part C: applications and reviews. Transactions on IEEE, 41, 494–508, 2011.

[7] R Dubey, D Rathore, D Kushwaha, JP Maurya, “An empirical study of intrusion detection system using feature reduction based on evolutionary algorithms and swarm intelligence methods”, International Journal of Applied Engineering Research 12 (19), 2017. pp. 8884-8889.

[8] D. Kong, J. Gong, S. Zhu, P. Liu and H. Xi. SAS: semantics aware signature generation for polymorphic worm detection. InternationalJournal of Information Security, 50, 1–19, 2011.

[9] Deepak Kumar Rathore, Praveen Kumar Mannepalli, “Recent Trends in Machine Learning for Health Care Sector”, International Journal of Innovative Research in Technology and Management, Vol-5, Issue-2, 2021.

[10] M. Sharma and D. Toshniwal. Pre-clustering algorithm for anomaly detection and clustering that uses variable size buckets. Recent Advances in Information Technology, 515–519, 2012.