International Academic Institute for Science and Technology

International Academic Journal of Science and Engineering
Vol. 7, No. 2, 2020, pp. 38-42.

ISSN 2454-3896

International Academic Journal of Science and Engineering

www.iaiest.com

Effective Intrusion Detection Through Anomaly Analysis

Vinit Mehra [a], Anjali Patel [b]

[a] *Department of Civil Engineering, Green Valley Institute of Infrastructure, Kochi, India.*
[b] *Department of Civil Engineering, Green Valley Institute of Infrastructure, Kochi, India.*

Abstract

Modern Internetworked systems put greater emphasis on Network Security. The growth of the internet and our growing dependence on it have raised the demand for network security technologies. Networking and Interoperability have grown better on public networks, which has caused a significant rise in the number and severity of security threats. To safeguard the frameworks, several Intrusion Prevention techniques have been developed. Authorization, user authentication, fixing coding and design errors, firewalls, and data protection are a few of the methods. These techniques are used to safeguard computer networks. Therefore, intrusion prevention alone would not be enough due to the system's increasing complexity. Security flaws in system design are common. Numerous variables, including flawed system configuration, inappropriate system behaviour, and errors in programming and design, contribute to these problems. Ineffective efforts are made by security regulations to meet system control and information access An Intrusion Detection System is widely used in systems to protect them IDS is to find organizations that are trying to bypass already-in-place security protections. These intrusions involve threats of imminent infractions of computer security regulations, standards, or established security processes.

Keywords: Intrusion Detection Systems, Deep Learning, attacks, classification,

Received: 19 September 2020/Revised: 30 October 2020/Accepted: 13 November 2020/Published: 31 December 2020

Introduction

Cloud computing is a new concept that provides a lot of computing resources and facilities to give cloud consumers the features they want through the Internet. Because cloud computing involves sensitive data, data maintenance is the key worry. Many companies wish to transfer a vast amount of data to the public cloud. The confidential data uploaded into cloud is exposed to risk of security, comprising integrity, confidentiality and availability of those sectors [1]. In addition to this, the unceasing services of cloud bring intruders to access, misuse resources and services offered by cloud service provider. There are various attacks that influence the privacy of services and resources of cloud within cloud computing system. Cloud computing is a business strategy for selling computing resources and services as well as a technology enabling more effective use of computing infrastructures. However, their dispersed and intricate architectures make them a desirable target for hackers. Cloud computing has a lot of potential to lower expenses and increase productivity, but it also comes with a lot of new security dangers [2]. Intrusion Detection Systems (IDS) have been widely used to detect malicious activity in hosts and network traffic. It is defined as a computer network system for collecting data on several key topics and evaluating that data to see if there are indications of an attack or violations of network security policy behaviour. Because cloud computing is distributed, the traditional intrusion detection system is not flexible enough to guarantee security in this environment. The majority of businesses are currently moving their computer services to the cloud. This enables people to readily access their computer processes. In terms of safety and dependability, it also presents new security threats. Because cloud computing is a "network of networks" over the internet, there is a considerable risk of intrusion due to the sophistication of the assaults used by hackers. Because cloud computing is decentralized, there is a significant chance of intrusion. It's crucial to research various intrusion detection and prevention strategies. To stop harmful attacks in traditional networks, various IDS techniques are used [3].

Need of the Study

IDS applies the Misuse Approach and the Anomaly Approach to scan communications for intrusion. The clearly established patterns (or signatures) possessed by IDS systems that are based on abuse detection often may be found by patterns of pattern recognition learned from training sets. It often reduces the level of false positives, although this is not always so. Misuse-based IDSs, like antivirus software, are unable to identify novel attacks or other threats that system administrators are unaware of. A misuse-based IDS needs to regularly update its signature sets in order to be effective [4-5]. Intrusion detection systems (IDS) are systems that employ anomaly detection to find intrusions. They are found by setting a baseline for the system under observation and identifying notable departures from it. Establishing an anomaly-based IDS with a limited definition of normal will also result in a sizable proportion of false-positives. It can also identify emerging threats, in contrast to IDS, which is usage-oriented. Depending on the data source, IDSs are categorized as either host-based or network-based. The Network-based intrusion detection system (NIDS) uses unfiltered network data packets as a data source and looks for indications of intrusions. NFR, Dragon, ISS, Snort, Bro, and Cisco Secure IDS are a few types of NIDS. Operating system audit trails (HIDS) and other data gathered from a particular computer network are used by host-based intrusion detection systems (IDS). System logs and C2 audit logs [6]. A common misconception is that firewalls can detect and eliminate intruders. The firewall is also a gate to control access to network destination points. IDS can provide a second layer of security to systems such as firewalls by detecting attacks that are feasible against them. The internet is essential to the ongoing communication of modern society, but its effectiveness can also reduce the impacts known as intrusions. Any action that negatively affects the targeted system is considered an intrusion. The availability of resources, confidentiality, and integrity of the compromised computer system can all be jeopardized by an incursion. An incursion compromises the security of a computer system. Among the attacks are network intrusions and host breaches. Host intrusions are defined as unauthorized attempts to alter access, alter, or remove data, or to cause instability or make the system unusable [8]. These work together to alter the system's state through malware, file system modification, privilege escalation, system call manipulation, Trojan horse, virus, and worm-induced unauthorized logins, and access to private data.

Methodology

Three delivery methods are used in cloud computing to offer end users different kinds of services. SaaS, PaaS, and IaaS are the three delivery models that provide consumers with software, application platforms, and infrastructure resources as services. Additionally, these models impose different security requirements on the cloud environment. PaaS and SaaS are built on top of Infrastructure as a Service (IaaS), which serves as the foundation for all cloud computing services. Information security risks and issues are inherited, much like capabilities. Each architecture has significant built-in feature, complexity versus extensibility, and security trade-offs. Customers will be held more

responsible for implementing and maintaining security features if the cloud service provider only guarantees security at the lower end of the security architecture. Machine learning has developed rapidly in new methodologies and applications in different intrusion detection setups in the last few years. As there are more variables in the dataset, the modern methods require more computationally intensive tasks, which deteriorates their accuracy. It is important to minimize the number of features by selecting qualities that are tolerable in order to enhance algorithm speed and accuracy. Feature selection grows faster as machine learning is a practically oriented discipline where research questions are increasingly being prompted by actual datasets. Since IDS lacks the ability to handle unknown attacks, machine learning that can scan bulk data is discarded for improved detection of some unknown attacks in IoT.

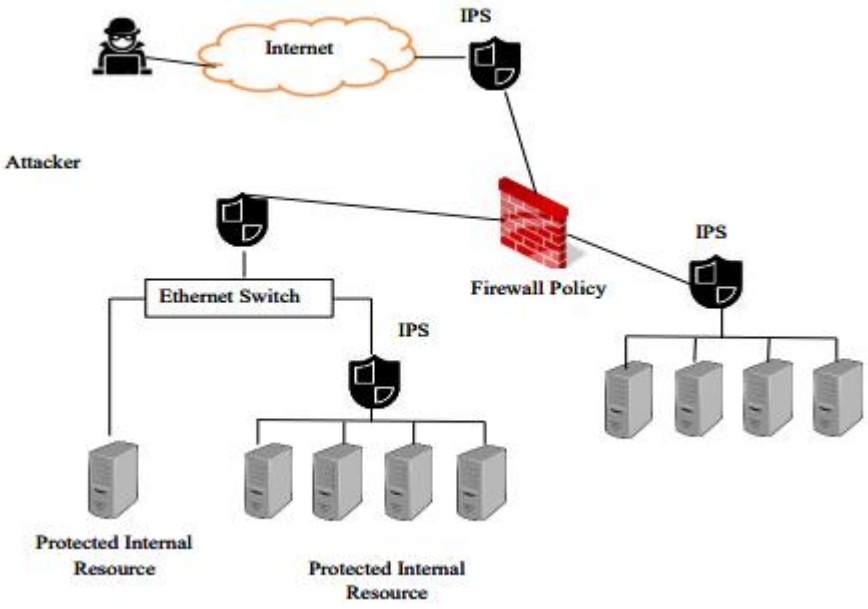

Figure 1: IDS prevention system

By examining changes in network traffic, end user behavior, and system configuration, intrusion detection systems identify hostile activities within a system. The system notifies the user or monitoring console to take steps to prevent such assaults if it detects malicious behavior of this kind. Researchers in the past have created intrusion detection systems based on the idea of conventional techniques such as support vector machines, fuzzy clustering, genetic algorithms, artificial neural networks, and association rule mining, which are not producing the best results in terms of false negative rates and detection rates. We developed a hybrid classification-based intrusion detection and prevention system for cloud environments in order to address these problems. In order to detect system intrusions, we introduced two new algorithms in this system: packet examination and the NK-RNN method, a hybrid classification model that combines the Nearest K-means algorithm with Recurrent Neural Network. Cloudlet Controller (CC), Trust Authority (TA), and Virtual Machine Manager are the components of our suggested solution, which focuses on intrusion detection and prevention mechanisms to identify questionable activities in cloud environments. According to our system design, the cloud's users are dispersed throughout the environment. When packets from many users are collected, network traffic will be present. By using Cloudlet Controller to collect packets from various users via a router, we were able to resolve this issue. When a cloudlet reaches its threshold, CC receives the packets and forwards them to other cloudlets that are not using them. As a result, network traffic is decreased, and it is very helpful to identify intrusions in an easy manner.

Experimental Results

By considering specific performance measures, experimental evaluation of the suggested work provides improved results when compared to other existing efforts. The suggested algorithm is evaluated using performance measures

such as F-score, false alarm rate, detection rate, packet loss ratio, speedup ratio, and throughput in order to assess the suggested hybrid classification-based intrusion detection and prevention approach.

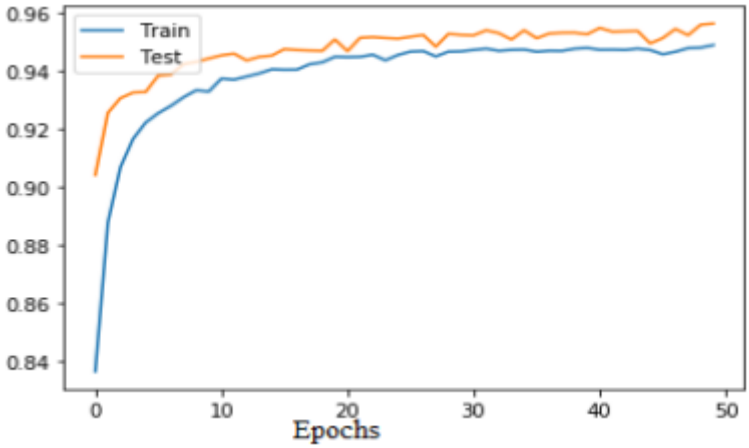

Figure 2: Accuracy of proposed model

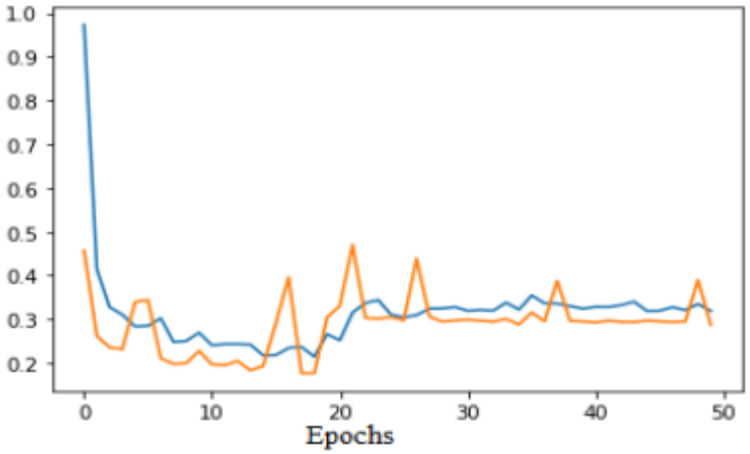

Figure 3: Loss of proposed model

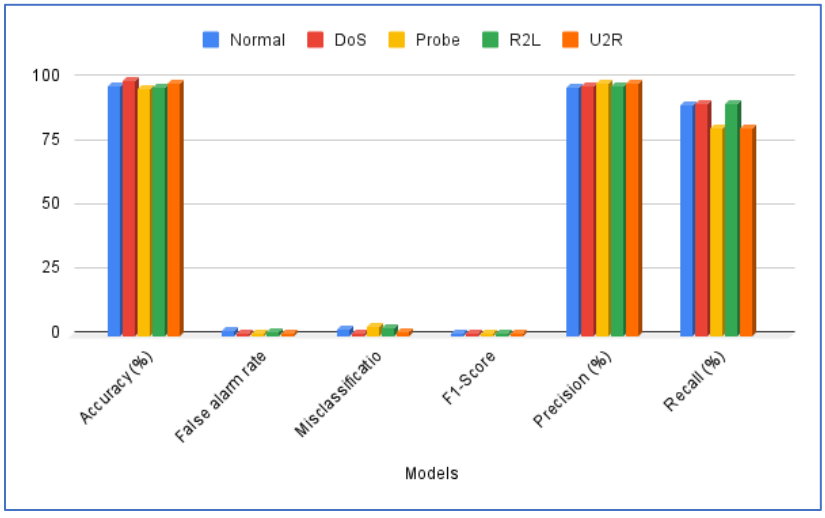

Figure 4: Performance metrics of HD detection

the key designers of the recommended cloud-based intrusion detection system. The proposed work uses the public IDS dataset, known as the KDD dataset, to test the IDS system using these implemented system elements. Using their names that were present in the dataset, packets were taken from entities. The dataset mentioned above is specifically provided to help identify any intrusions in the system. There are four types of attacks in the dataset: DoD, R2L, U2R, and probing. Although it is not limited, the current study listed some of the dataset's most notable properties. The characteristics can be either continuous or discrete. Performance criteria such F-Score, false alarm rate, detection rate, speedup ratio, packet loss ratio, and throughput were taken into account when analyzing the suggested system's performance. The comparison analysis's findings show that our suggested method is more effective in identifying intrusions in cloud systems.

Conclusions

Today, every organization prefers Cloud computing because it is very flexible and scalable. But privacy and security is the top concern as it has open and distributed architecture. Cloud computing offers good quality service and secure the user's confidential data. Attackers can target end users' private information, storage capacity, bandwidth, and processing capacity of the cloud network due to the distributed nature of cloud computing systems. The network's availability, secrecy, and integrity are destroyed by intrusion assaults such as DDoS, floods, R2L, U2R, and probing. The network's permission, authentication, and security are all at risk from these assaults. The majority of external attacks are prevented by traditional network security channels like firewalls; however, they are not suitable for detecting sophisticated external attacks or insider threats. An intrusion detection system is suggested as a solution to these problems in order to detect network attacks. It can provide additional security measures in a distributed cloud setting.

References

Nadiammai, G. V., & Hemalatha, M. J. E. I. J. (2014). Effective approach toward Intrusion Detection System using data mining techniques. *Egyptian Informatics Journal*, *15*(1), 37-50. https://doi.org/10.1016/j.eij.2013.10.003

Kachirski, O., & Guha, R. (2003, January). Effective intrusion detection using multiple sensors in wireless ad hoc networks. In *36th Annual Hawaii International Conference on System Sciences, 2003. Proceedings of the* (pp. 8-pp). IEEE. https://doi.org/10.1109/HICSS.2003.1173873.

Jyothsna, V. V. R. P. V., Prasad, R., & Prasad, K. M. (2011). A review of anomaly based intrusion detection systems. *International Journal of Computer Applications*, *28*(7), 26-35.

Jabez, J., & Muthukumar, B. J. P. C. S. (2015). Intrusion Detection System (IDS): Anomaly detection using outlier detection approach. *Procedia Computer Science*, *48*, 338-346. https://doi.org/10.1016/j.procs.2015.04.191

Gogoi, P., Borah, B., & Bhattacharyya, D. K. (2010). Anomaly detection analysis of intrusion data using supervised & unsupervised approach. *J. Convergence Inf. Technol.*, *5*(1), 95-110. https://doi.org/10.4156/jcit.vol5.issue1.11

Aljawarneh, S., Aldwairi, M., & Yassein, M. B. (2018). Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. *Journal of Computational Science*, *25*, 152-160. https://doi.org/10.1016/j.jocs.2017.03.006

Gupta, S. (2015, October). An effective model for anomaly IDS to improve the efficiency. In *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)* (pp. 190-194). IEEE. https://doi.org/10.1109/ICGCIoT.2015.7380455.

Erbacher, R. F., & Sobylak, K. (2002, September). Improving intrusion analysis effectiveness. In *2002 Workshop on Computer Forensics*.