International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 8 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT183878

Implementation of Hybrid Approach for Intrusion Detection in Cloud Computing Environment

Preeti Chourasiya
Department of Information Technology, PCETs Pimpri Chinchwad College of Engineering, Pune, Maharashtra, India

ABSTRACT

Cloud computing is a very fast growing technology that offer novel service to the Information Technology domain. With the help of cloud computing will reduce the infrastructure maintenance cost. The probability of having numerous types of vulnerabilities beginning attacks is high. In this paper we study and analysis dissimilar approach of an intrusion detection system that has been utilize to counter malicious attacks in Cloud computing environment. In this paper we implementation of hybrid approach for intrusion detection in cloud computing environment. The proposed approach based on ANN with fuzzy logic based Hybrid IDS, to which is additional proficient than the traditional IDS (Intrusion Detection System).

Keywords: Cloud Computing, IDS, ANN, fuzzy logic, DoS, DDoS.

I. INTRODUCTION

Today, numerous organizations are moving their computing services just before the Cloud. However, they can access in an accessible method to a lot of online services deprived of having to achieve the essential infrastructure that is frequently complex. Cloud computing has also three service models specifically Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS) models. IaaS model delivers services to customers by preserving huge infrastructures like hosting servers, running networks and other resources for clients. Essentially, the IDS have been implemented in groups to accumulate and analyse numerous types of attacks within a host system or a network. In addition, to classify and detect probable threats violations, which include both intrusions, which are the attacks after outside the organizations and misuses that are recognised as the attacks within the organizations. In this research work, to propose the hybrid which includes a mixture of the two systems Intrusion Detection. Different IDS approach are used to counter malicious attacks in traditional networks. For Cloud computing, huge network access rate, renouncing the control of data & applications to service supplier and distributed attacks vulnerability, an effective, reliable and information transparent IDS is essential. Through fuzzy clustering technique, the various training set is divided to numerous homogenous subsets. Thus

Complexity of every sub training set is compact and subsequently the detection performance is incusing dataset deliver efficiency of our novel hybrid technique for low frequent attack In this research, how to conclude the suitable number of clustering remains an open problem. Furthermore, other data mining approach, such as support vector machine, evolutionary computing, outlier detection, may be presented into IDS. Evaluation of numerous data mining approach will provide clues for constructing additional effective hybrid approach for detection intrusions in cloud network.

The existing IDS deployed in traditional Internet lack the features of autonomic self-adaptation and scalability. In adding, they are not deterministic which variety them inappropriate for cloud based environments. This urges the essential of a novel cloud based IDS which can transfer out its security requirements.

In this paper we implementation of hybrid approach for intrusion detection in cloud computing environment. The proposed approach based on ANN with fuzzy logic based Hybrid IDS, to which is additional proficient than the traditional IDS (Intrusion Detection System). The rest of this paper is structured as follows: In section II, we designate concisely numerous probable intrusions in Cloud. Section III presents detection approach used by IDS. In Section IV, we describe different types of IDS in Cloud. Presents detailed analysis of numerous existing IDS techniques for cloud. Section VI achieves our work with the references at the end.

II. RELATED WORK

Numerous efforts have been taken in the extent of Cloud computing and IDS but still there are additional attacks that have not been detected.

Shaikh et al[1]providers can be eliminated by using Host-Based IDS. Examine that the use of Virtual Machines snapshot as an evidence, encompasses additional storage and similarly time consuming than the log gathering by Intrusion Detection System.

Luan Huy Pham et al[2]proposed a quantitative risk valuation framework for adaptive intrusion detection to address APTs in the cloud and, additional usually, any target attacks employing a multitude of attack mechanisms transversely dissimilar subsystems. In the cloud landscape, the proposed framework can be accepted at dissimilar levels of abstraction.

Q. Xia et al[3] design a hybrid sampling scheme. In this design, expending a grouping of local and global sampling decisions, author proposed a technique filter out numerous packets and yet maintain detection accuracy, construction unmodified traditional IDS operating in a cloud environment. To proposal an SDN-based packet group and monitoring mechanism that permits proficient packet collection after inside a cloud.

Y. Mehmood et al[4] developed a hypothesis including two questions: how can we efficiently use mobile agents to perceive the distributed intrusions in cloud and what is the consequence of correlation in intrusion detection procedure from cloud perspective

A. Aborujilah et al[5] Numerous of the IDS are located separate of the virtual network, so, the flooding attacks occurred inside the virtual network cannot be detected. Numerous of the cloud IDS technique need using one IDS instance in every VM in the virtual network. This thoughtful of detection technique consumes the resource intensively.

III. PROPOSED METHODOLOGY

The proposed IDS are Hybrid technique for improving the performance of traditional IDS systems. The proposed model is demonstrated using dataset for classifying the attack classes. Therefore first the dataset is accepted as input to the proposed system and then the pre-processing on data is performed for eliminating the missing value issues. In next the data is encoded to provide similar set of data. In next the correlation coefficient based feature selection technique is used for reducing the dimensions of data. Finally the entire data is sub-divided into two parts training data and testing data. The 65% of data is used for training purpose and 35% of data is used for testing purpose. After that the fuzzy clustering technique is trained with the selected features set and

the testing with the testing set is performed. Trained model: after training using the input training dataset which are the composition of selected feature attributes and the classes (attack types) the returns the model. That model help to accept the fuzzy clustering test dataset which is in format of unlabelled patterns and for each pattern the trained model return the class labels. The test dataset is unlabelled data which is produced to the trained model for identifying the class labels of the input pattern. In the similar manner the features of test dataset without classes are produced in previous step to predict the classes of input pattern or the attack pattern. Based on the outcome of classification the performance is computed in terms of accurately classified pattern. After classification of the test dataset which is randomly selected from the initial dataset the performance of the classification is computed. The classification performance is defined in terms of accuracy, error rate and the consumed resources. Based on the experimentation the performance of the system is concluded. The implementation of the proposed technique is performed on JAVA technology. After design and implementation the performance of the system is computed in terms of different performance factors which are summarized. According to the given performance evaluation the performance of the proposed technique is efficient as compared to the traditional technique classification technique. Furthermore necessitates less time and memory for classifying the samples. Thus the proposed hybrid is suitable for effective intrusion detection methodology. The simulation experiment consequences illustration that this method can successfully expand the detection efficiency of the attack data, and has good applied value. The test dataset adopts the is intended for anomaly based systems. The quantity of traces collected from for every category for dataset is described. They using to produce dataset of system call traces for precise development an auditing utility for gathering security applicable events. The dataset was collected under Ubuntu 16.04 fully patched operating system through kernel 2.6.38. The operating system was running dissimilar services, Apache running java, MySQL, SSH server, FTP server etc. similarly joins system call traces of dissimilar types of attacks. Describes specifics of every attack class in dataset. This dataset can somewhat simulate the definite cloud environment in runtime. In instruction to estimate the consequence of the detection system, it uses the consequent indicators, with the false positive rate, false negative rate, detection time, etc. It is distinct as follows:

False positive rate= (Number of attack traces detected as normal traces) / total number of normal traces.

Detection rate = (Number of intrusion traces have been detected) / total number of traces.

It is a graph of true positive rate in contradiction of false positive rate. It signifies the performance of binary classifier as its discernment threshold is varied. To test the performance of the technique, we use standard approach and improved fuzzy clustering algorithm at the similar time to associate the detection algorithms. The performance of the hybrid approach in terms of accuracy is given in this section. The performance evaluation of proposed Intrusion detection system is evaluated using implementation of coefficient correlation analysis.

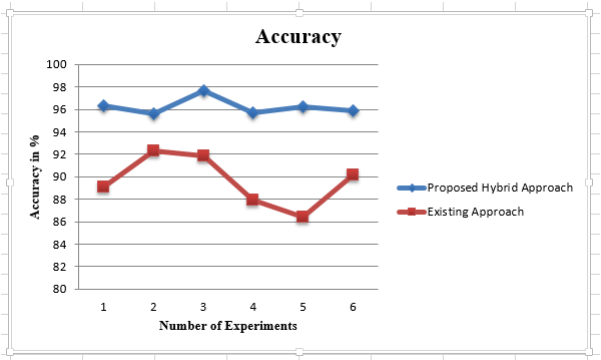

Figure 1 : Compare Accuracy proposed approach and existing approach

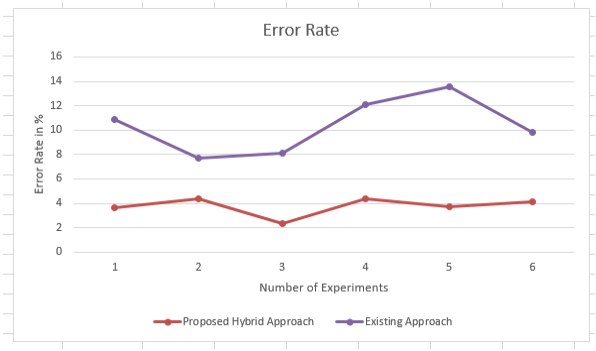

Figure 2 : Error Rate

The data consequences comparison among false positive rate and detection rate. From the comparison accuracy, it can be seen that enhanced bisecting existing technique method has improved detection results. The experimental consequence dataset demonstrates the effectiveness of our novel approach especially for low-frequent attacks, attacks in interactions of detection precision and detection stability. Additional self-determining and compacted, the cluster can converge speedily and acquire improved recognition outcomes. Standard fuzzy clustering has dissimilar result in different value, and it is easy to fall into local optimum, affecting the detection outcomes. While the better intersecting method does not differentiate features of high-dimensional data, subsequent in quantity of the comparable data affecting the detection rate and false alarm rate.

IV. CONCLUSION

In this presented work the cloud computing application in intrusion detection system is provided. Additionally the two key issues are targeted for finding the effective and efficient solution. The primary aim is to find the suitable features set from the entire dataset. That helps to reduce the dominations of data and scale the processing speed of the IDS system. On the next improve the classifier performance for classifying the multiple class data. Therefore to resolve this issue the ANN based on fuzzy technique is used for performing training and testing using the Fuzzy logic. Using the two discussed improvements the a new approach is proposed for implementation and design that claims high performance in terms of processing speed and the efficient outcomes in terms of accurate results.

V. REFERENCES

[1]. A. A. Shaikh, H. Qi, W. Jiang and M. Tahir, "A novel HIDS and log collection based system for digital forensics in cloud environment," 2017 3rd IEEE International Conference on Computer and Communications (ICCC), Chengdu, 2017, pp. 1434-1438. doi: 10.1109/CompComm.2017.8322779

[2]. Luan Huy Pham, M. Albanese and S. Venkatesan, "A quantitative risk assessment framework for adaptive Intrusion Detection in the cloud," 2016 IEEE Conference on Communications and Network Security (CNS), Philadelphia, PA, 2016, pp. 489-497. doi: 10.1109/CNS.2016.7860540

[3]. Q. Xia, T. Chen and W. Xu, "CIDS: Adapting Legacy Intrusion Detection Systems to the Cloud with Hybrid Sampling," 2016 IEEE International Conference on Computer and Information Technology (CIT), Nadi, 2016, pp. 508-515. doi: 10.1109/CIT.2016.31

[4]. Y. Mehmood, M. A. Shibli, A. Kanwal and R. Masood, "Distributed intrusion detection system using mobile agents in cloud computing environment," 2015 Conference on Information Assurance and Cyber Security (CIACS), Rawalpindi, 2015, pp. 1-8. doi: 10.1109/CIACS.2015.7395559.

[5]. Aborujilah and S. Musa, "Critical review of intrusion detection systems in cloud computing environment," 2016 International Conference on Information and Communication Technology (ICICTM), Kuala Lumpur, 2016, pp. 251-255. doi: 10.1109/ICICTM.2016.7890809

[6]. X. Zhao and W. Zhang, "An Anomaly Intrusion Detection Method Based on Improved K-Means of Cloud Computing," 2016 Sixth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC), Harbin, 2016, pp. 284-288. doi: 10.1109/IMCCC.2016.108.

[7]. H. Hammami, H. Brahmi and S. Ben Yahia, "Security insurance of cloud computing services through cross roads of human-immune and intrusion-detection systems," 2018 International Conference on Information Networking (ICOIN), Chiang Mai, 2018, pp. 174-181. doi: 10.1109/ICOIN.2018.8343106

[8]. Z. Chiba, N. Abghour, K. Moussaid, A. El Omri and M. Rida, "A survey of intrusion detection systems for cloud computing environment," 2016 International Conference on Engineering & MIS (ICEMIS), Agadir, 2016, pp. 1-13. doi: 10.1109/ICEMIS.2016.7745295

[9]. X. Zhao and W. Zhang, "Hybrid Intrusion Detection Method Based on Improved Bisecting K-Means in Cloud Computing," 2016 13th Web Information Systems and Applications Conference (WISA), Wuhan, 2016, pp. 225-230. doi: 10.1109/WISA.2016.

[10]. H. C. Liu, X. N. Hou, Z. Yang, “Design of Intrusion Detection System Based on Improved Kmeans Algorithm,” Comput. Technol. Dev., vol.26, no.1, Jan.2016. [22] S. Harifi, E. Byagowi, and M. Khalilian, “Comparative Study of Apache Spark MLlib Clustering Algorithms,” In Proc. Int. Conf. Data Min. Big Data, pp.61-73, Jul.27-Aug.1, 2017.

[11]. M. K. Siddiqui, S. Naahid, “Analysis of KDDCUP 99 dataset using clustering based data mining,” Int. J. Data Theory Appl., vol.6, no.5, pp. 23-34, June.2013.

[12]. S. Madan, K. J. Dana, “Modified balanced iterative reducing and clustering using hierarchies (m-BIRCH) for visual clustering,” Pattern Anal. Appl., vol.19, no.4, pp.1023-1040, Nov.1, 2016.