Gyanshauryam, International Scientific Refereed Research Journal
© 2019 GISRRJ | Volume 2 | Issue 6 | ISSN : 2582-0095

An Efficient Virtual Machine Intrusion Detection System on Cloud Computing

Sathiya Dharani K, Akilandeswari K
Department of Computer Science, SJSV CAS, Coimbatore, Tamil Nadu, India

ABSTRACT

As Cloud Computing is the rapidly growing field of IT. Cloud Computing is defined as an Internet based computing in which virtually shared servers that is data centers provide software, platform, infrastructure, policies and many resources. In this research we have analyzed, the various intrusion log files of virtual machines in order to identify the significant features for creation of intrusion model. In this research we have used logistic regression classification algorithm. Through this algorithm we have achieved the highest accuracies with low false positive rate.

Keywords : IDS, Virtual Machine, Logitboost, Accuracy, Cloud Environment.

I. INTRODUCTION

Cloud computing is not just a joining to something over the internet. In its place, it is re-imagination of an outmoded data center. Data midpoint constituents like Servers, Storage and Networking are accomplished separately. Cloud Computing allows well-organized use of capitals in a data center by allocation it through diverse examples of calculate. It also empowers users to establishment the resources themselves [1]. It will be talented to effortlessly scale up or balance down the possessions which they requirement on demand. Cloud resources are adaptable; contingent on the load to a specific instance, calculate possessions like RAM, CPU can be additional on call so that the illustration does not bang.

National Institutes of Standards and Technology (NIST) describes whatever cloud computing is and what are the cloud computing prototypes. Cloud computing is a developing technology determined by the requirements for flexible IT arrangement, the appearance of big data analytics and enlarged mobile usage. Cloud computing is a knowledge which everything only on the internet; central distant servers are used to sustain data and applications [2]. Cloud computing permits the users to use applications deprived of installing software's. The users can admission the internet and send messages wherever in the world. Cloud computing permits more well-organized computing by central storage, memory, dispensation and bandwidth. The greatest example is Google mail. For this, the users essential not install any software or a server to use a Google mail explanation. The user can admission internet, over which he sends messages [3]. Consequently the servers and email software are all contemporary on the cloud i.e. internet and these software's and servers are accomplished by the cloud service breadwinner i.e. Google.

Cloud computing is separated in to three layers, structure, software and policy.

GISRRJ19267 | Received: 01 Nov 2019 | Accepted: 29 Nov 2019 | November-December-2019 [2 (6) : 24-27]

II. RELATED WORK

In [4] the authors developed an IDS approach based on cloud that interconnects to host cloud via a virtual private network (VPN). The host cloud and the IDS cloud are in an interpenetrating architecture within whole cloud infrastructure. In host and IDS sides of the VPN connection, there are proxies which transfers data between IDS and the host clouds. User Data Collector collects data from host cloud behind the host side proxy and IDS side proxy receives these data, and sends them to analyze engine of the IDS. Then analyze engine inspects the instances with user information and signature database.

In [5] the authors concluded Snort is much better and has some pluses than other NIDS. Snort is not commercial, and it is under General Public License (GPL). So a Snort user has not to pay amounts of dollars to implement it to a network. And also administration of the Snort is smoother than other on the shelf NIDS that is under either GPL or commercial.

In [6] introduced an unrealized cloud based IDS that runs in an isolated environment within public cloud in the PaaS level. A user has the whole control of the IDS and the provider has no responsibility on the intrusion detection mechanism. It can define VPNs between sub clouds or different clouds, which are founded in discrete geographical locations. IDS SaaS supports many cloud features as portability, elasticity, scalability and for the most important point on demand access.

III. PROPOSED SYSTEM DESIGN

The proposed intrusion detection framework begins with the collecting the event level log files from the virtual machine monitor as shown in the figure 1. Once the event level log files are collected, the collected event log files analyzed in terms of their characteristics and statistical behavior in order to identify the significant features for the detecting the intrusion in cloud virtual machine monitoring systems. Once the significant features are identified, the learning model should be created to classify the given event log profile features. The outcome of the model is to classify whether the given event log profiles are intrusion or normal profile.

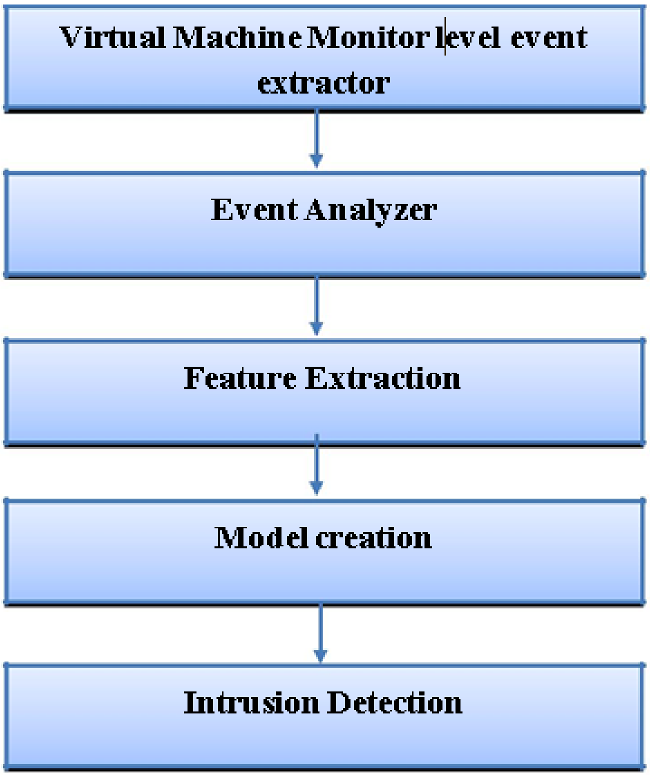

Figure 1. Proposed Intrusion detection system framework

The intrusion detection experiments are conducted using Weka data mining tool. Weka tool is an open source investigation tool for organization and clustering algorithms. The proposed research work utilizing the logitboosting classification algorithm for identification of the intrusion detection in the cloud environment. To estimate the performance of the suggested work utilized four dissimilar measures namely, precision, recall, accuracy and false positive rate.

Estimated our classifier with various calculation measures, such as accuracy, F-measure and false positive rate.

Accuracy is percentage of correctly identified intrusion log profiles.

$$\text{Accuracy}= \frac{TP+TN}{TP+FP+FN+TN}$$

True Positive (TP) =Number of samples correctly predicted as intrusion log profiles.

False Positive (FP) = Number of samples incorrectly predicted as intrusion log profiles.

True Negative (TN) = Number of samples correctly predicted as benign log profiles.

False Negative (FN) = Number of samples incorrectly predicted as benign log profiles.

Precision is a measure of what fraction of test data is detected as intrusion log profiles are actually from the intrusion log profile classes.

$$\text{Precision (P)} = \frac{TP}{TP + FP}$$

Recall measures the fraction of intrusion log profiles class that was correctly detected.

$$\text{Recall (R)} = \frac{TP}{TP + FN}$$

False Positive Rate (FPR) is percentage of wrongly identified benign log profile classes.

$$\text{Positive Rate (FPR)} = \frac{FP}{FP + TN}$$

The experimental results are given in table 1.

Measures	**Values**
Precision	0.980
Recall	0.979
Accuracy	97.90
False Positive Rate	0.009

Table 1. Experimental results of LogitBoost Classifier

From the table, one can confirm that the LogitBoost classifier attains highest accuracy of 97.90% and false positive rate of 0.009 when detecting the intrusion in the cloud environment.

IV. CONCLUSION

In this research, we have presented data mining based intrusion detection system virtual machine monitoring in cloud environment. The system starts with investigating the statistical behavior of virtual machines, then gratitude of important features and applied data mining method to categorize the event log profile data into intrusion profile and benign profile. Through LogitBoost classifier achieved 97.90% accurateness.

V. REFERENCES

[1]. Ghosh, P., Bardhan, M., Chowdhury, N. R., & Phadikar, S. (2017). IDS Using Reinforcement Learning Automata for Preserving Security in Cloud Environment. International Journal of Information System Modeling and Design (IJISMD), 8(4), 21-37.

[2]. Gupta, D., & Gupta, S. (2017, October). An efficient approach of trigger mechanism through IDS in cloud computing. In Electrical, Computer and Electronics (UPCON), 2017 4th IEEE Uttar Pradesh Section International Conference on (pp. 68-72). IEEE.

[3]. Deshpande, P., Sharma, S. C., Peddoju, S. K., & Junaid, S. (2018). HIDS: A host based intrusion detection system for cloud computing environment. International Journal of System Assurance Engineering and Management, 9(3), 567-576.

[4]. Baraka, H. B., & Tianfield, H. (2014, September). Intrusion detection system for cloud environment. In Proceedings of the 7th International Conference on Security of Information and Networks (p. 399). ACM.

[5]. Singh, D., Patel, D., Borisaniya, B., & Modi, C. (2016). Collaborative ids framework for cloud. International Journal of Network Security, 18(4), 699-709.

[6]. Damopoulos, D., Kambourakis, G., & Portokalidis, G. (2014, April). The best of both worlds: a framework for the synergistic operation of host and cloud anomaly-based IDS

for smartphones. In Proceedings of the Seventh European Workshop on System Security (p. 6). ACM (2) please write your biography and academic details.

Cite this article as :

Sathiya Dharani K, Akilandeswari K, "An Efficient Virtual Machine Intrusion Detection System on Cloud Computing", Gyanshauryam, International Scientific Refereed Research Journal (GISRRJ), ISSN : 2582-0095, Volume 2 Issue 6, pp. 24-27, November-December 2019.
URL : http://gisrrj.com/GISRRJ19267