Virtual Intrusion Detection System Using Cloud Computing

Aparna Shukla[1], Keertana LN[2], Manoj Kumar MC[3], Kavya DN[4]
[1, 2, 3] Dept of Computer Science and Engineering
[4]Professor, Dept of Computer Science and Engineering
[1, 2, 3, 4] Atria Institute of Technology, Bangalore, Karnataka, India

Abstract- *Intrusion is act of wrongfully entering, seizing and taking possessions.Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user.The term is generally used to describe data centres available to many users over the Internet. In this paper, we make use of log files taken from cloud in order to extract important features for developing an intrusion detection model. In this research we have used Random forest, KNN and Naïve Bayes algorithms. By using these algorithms, we calculate and achieve highest accuracies.*

Keywords- Intrusion Detection System, Cloud, KNN, Random Forest, Naïve Bayes.

I. INTRODUCTION

Cloud computing is basically, companies renting access to anything from application to storage from a cloud service provider. One benefit of using cloud computing services is that firms can avoid the upfront cost and complexity of owning and maintaining their own IT infrastructure, and instead simply pay for what they use, when they use it.In turn, providers of cloud computing services can benefit from significant economies of scale by delivering the same services to a wide range of customers.Cloud computing services cover a vast range of options now, from the basics of storage, networking, and processing power through to natural language processing and artificial intelligence as well as standard office applications. Pretty much any service that doesn't require you to be physically close to the computer hardware that you are using can now be delivered via the cloud. A fundamental concept behind cloud computing is that the location of the service, and many of the details such as the hardware or operating system on which it is running, are largely irrelevant to the user. Building the infrastructure to support cloud computing now accounts for more than a third of all IT spending worldwide, according to research from IDC. No more buying servers, updating applications or operating systems, or decommissioning and disposing of hardware or software when it is out of date, as it is all taken care of by the supplier. Using cloud services means companies can move faster on projects and test out concepts without lengthy procurement and big upfront costs, because firms only pay for the resources they consume.An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.

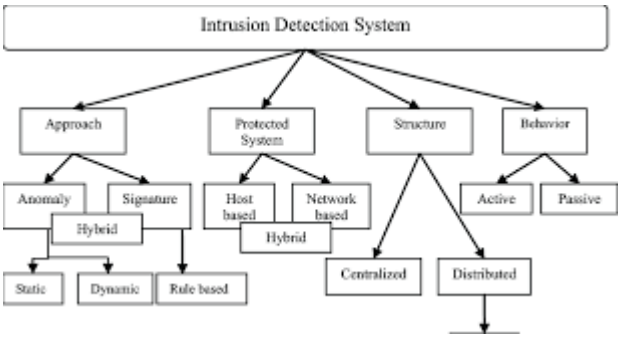

Fig1.Intrusion Detection System

Basically Intrusion Detection system is of five different types: Network Intrusion Detection System, Host Intrusion Detection System, Protocol Based Intrusion Detection system, Application Protocol Based Intrusion Detection System, Hybrid Intrusion detection. There are two ways to detect Intrusion: Signature Based Method and Anamoly Based Method.

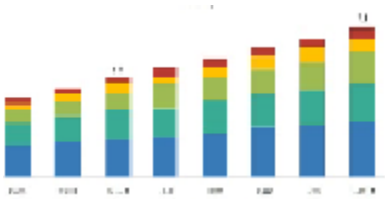

Fig 1. Intrusion Detection and Prevention byMarket

Worldwide spending on cyber security is forecasted to reach $133.7 billion in 2022.Data breaches exposed 4.1 billion records in the first half of 2019.Between January 1, 2005 and April 18, 2018 there have been 8,854 recorded breaches.

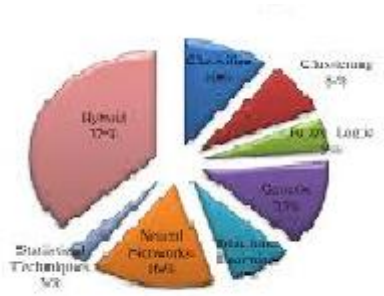

Fig 3.Result of Intrusion Detection System using different Techniques

II. LITERATURE SURVEY

[1] Ghosh, P., Bardhan, M., Chowdhury, N. R., &Phadikar, S. (2017). IDS Using Reinforcement Learning Automata for Preserving Security in Cloud Environment. In this paper they have incorporated Reinforcement Learning Automata with their proposed IDS while detecting and classifying attacks. Using learning automata an effective rule set is generated with the proposed algorithm from vast training set to improve the learning process at reduced computation cost and time. After which, the proposed reinforcement learning algorithm helps in classification of attacks accurately using the reinforcement signal. This proposed model was experimented with NSL-KDD as well as KDD 10% dataset and have proved its robustness by detecting attacks more accurately being an IDS. [2] Deshpande, P., Sharma, S. C., Peddoju, S. K., &Junaid, S. (2018). HIDS: A host based intrusion detection system for cloud computing environment, reports a host based intrusion detection model for Cloud computing environment along with its implementation and analysis. This model alerts the Cloud user against the malicious activities within the system by analyzing the system call traces. The method analyses only selective system call traces, the failed system call trace, rather than all. An early detection of intrusions with reduced computational burden can be possible with this feature. The reported model provides security as a service (SecaaS) in the infrastructure layer of the Cloud environment. Implementation result shows 96 % average intrusion detection sensitivity.[3] Baraka, H. B., &Tianfield, H. (2014, September). Intrusion detection system for cloud environment.IDS is designed to detect malicious node by using optimization and AI (Artificial Intelligence) techniques. The data is optimized using firefly algorithm. The firefly algorithm is a meta-heuristic approach which is inspired by the behavior of fireflies. The optimization algorithm helps to find the best feature. On the basis of extracted features the SVM (Support vector machine) is trained. SVM is a binary classifier which is used to solve multi-class problems. SVM is used to distinguish between attacker nodes and genuine nodes. Thus, instead of passing data to the attacker node, the node passes the data to the genuine node and hence, the system is protected. To know the performance of the system, QoS (Quality of service) parameters such as PDR (Packet delivery ratio), energy consumption rate and total delay with and without prevention algorithm are measured. The execution has been done in CLOUDSIM environment.

III. RELATED WORK

[4] Many approaches have been made on building an effective Intrusion Detection System. An approach has been made with the help of novel collaborative IDS framework for cloud, using snort to detect the known stealthy attack using signature matching. To detect unknown attacks, anomaly detection system (ADS) is built using Decision Tree Classifier and Support Vector Machine (SVM). Alert Correlation and automatic signature generation reduce the impact of Denial of Service (DoS) /Distributed DoS (DDoS) attacks and increase the performance and accuracy of IDS.

[5] Another approach is made using hybrid host/cloud IDS arrangement (as it assembles the best characteristics of both worlds) and to provide quantitative evaluation facts on if and in which cases machine learning-driven detection is affordable when executed on-device. Two main research issues are tackled: (a) the definition of an architecture which can be used towards implementing and deploying such a system in a dual-mode (host/cloud) manner and irrespectively of the underlying platform, and (b) the evaluation of a proof-of-concept anomaly-based IDS implementation that incorporates dissimilar detection features, with the aim to assess its performance qualities when running on state-of-the-art mobile hardware on the host device and on the cloud.

IV. PROPOSED SYSTEM

In the proposed system, we propose a novel deep learning model to enable NIDS operation within modern networks. In the process we use combination of deep and shallow learning. We use different machine learning algorithm to get the best accuracy. The system design is as follow:

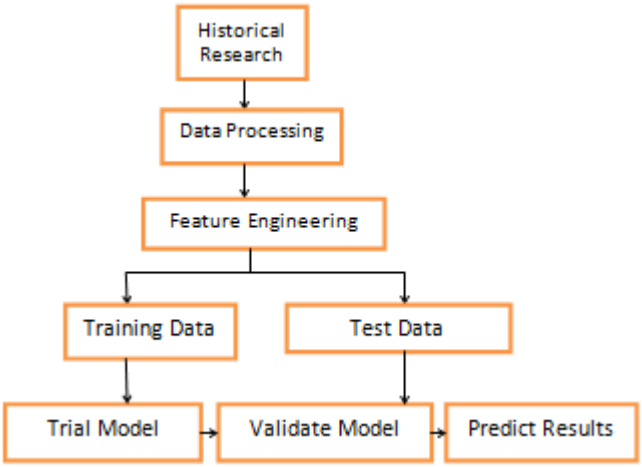

Fig 4. System Architecture

We imply KNN, Random Forest and Naïve Bayes. More specifically we combine the power of stacking our proposed Non-symmetric deep Auto-Encoder, and the accuracy and speed of Random Forest. The process starts by collecting data , we are using cloud to take files that we will need to examine. After that we perform operations on those files and record the behaviour. The main advantage of the proposed system is that it ensembles model predicts more accurate results, higher performance compared to existing system and more accurate and reliable results. There are 43 features on which every entry is tested. These 43 fields are divided as independent and dependent variable. 42 features are independent while the last one that is the result is based on other features , and called dependent features. We are using confusion matrix that contains four fields namely, true positive, true negative, false positive, false negative.

True Positive rate = TP/ (TP+ FN)
True Negative Rate = TN / (TN +FP)
Accuracy = TP+ TN / (TP+TN+FP+FN)
Precision = TP / (TP+FP)
Recall = TP / (TP+FN)

V. CONCLUSION

This paper provides a brief explanation of the process of designing an efficient virtual machine intrusion detection system using machine learning algorithms. Many models are there that have used standalone algorithms as well as hybrid models. In this approach we started with collecting data from cloud and using it to find similar behaviours. We calculate using all three algorithms namely KNN, Random Forest, Naïve Bayes. Naïve Bayes algorithm after performing all the calculation gives 30% accuracy which is the least. KNN after performing all the operations gives 95% accuracy which is more than Naïve Bayes. Random Forest gives 98% accuracy which is the highest among all three, and Random Forest is best suited for designing an efficient intrusion detection system.

VI. ACKNOWLEGEMENT

I would like to express my thanks to Dr. .Aishwarya P, Head of Department, Computer science and Engineering, Atria Institute of Technology, Bangalore for her consistent guidance that helped me to completing the dissertation successfully. I would like to especially thank my Project guide Prof. Kavya DN, Department of Computer Science and Engineering, Atria Institute of technology, Bangalore for her constant guidance and valuable advice, support and constructive suggestions.

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] 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.

[3] 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.

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

[5] 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.

[6] 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.