IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 10, Issue 1, January 2020, ||Series -III|| PP 40-44

A Novel Approach to Design the Intelligent Technique for Intrusion Detection In Cloud

Dr. Devendra P. Kale , Dr. V. M. Thakare
MCA Department Saraswati College Shegaon, India
P.G.Dept. of Comp. Science Faculty of Engineering & Technology SGBAU Amravati, India
Received 01January 2020; Accepted 15 January 2020

Abstract— In the cloud computing, security mechanisms are not mature enough to protect the data stored in the cloud. Hence, it is necessary to propose efficient methods for providing security to the data stored in the cloud. An intrusion detection system is dynamic software for cloud networks and databases that provides security for different network infrastructures and it can be extended easily. It is used to spot the mean users who violate their system privileges and become intruders. An intrusion detection system developed for securing the computer networks is monitored by the network traffic. In this paper, an Intrusion Detection System which is capable of identifying various kinds of attacks on cloud databases in public cloud is planned and executed. The intrusion detection is performed by proposing a new algorithm which has been designed and implemented by integrating Naïve Bayes classifier with Support vector Machines (SVM) using intelligent agents. The proposed system includes a new prevention module where prevention of intruders and malicious users are carried out using an intelligent decision manager that performs inference by sacking some rules.
Keywords— Security mechanism, Intrusion Detection System, cloud database, Support vector Machines.

I. INTRODUCTION

The Cloud Computing is the preferred choice of every IT organization since it proposes many desirable features to attract organizations to move their existing Information Technology assets toward the cloud [1]. As Cloud computing is a newly emerged technology, it is getting popularity day by day due to its amazing services [2]. The security and privacy is a major hurdle in its success because of its distributed architecture that is vulnerable to intruders. Regardless of the cloud deployment model, clouds provide one or more features to the end-users based on their applications domain. These choices are intended for rapid application development, self-managing workload adjustments, and financial cost savings. The following are some of the features that are promised by the cloud providers [3].

A. Elastic Scalability

Cloud users have the ability to modify the number of consumed resources based on their application demands. Thus, users with large data processing loads can divide them into smaller parts and distribute them into multiple tasks operated by on-demand cloud resources.

B. High Availability

For a complex environment like the cloud where large numbers of virtual resources are initialized, relocated, and cancelled based on customers on-demand requirements, the need to have a stable and reachable service is mandatory. The cloud promises the users with accessibility even when there are some failures on its assets. Individual services may fail for one or more particular users, but the system continues to survive for other services or different group of users.

C. Utility based Service

Cloud systems offer the financial concept of 'pay-as-you-go' subscription as their main billing system. In this module, customers get the functionality they need on a powerful infrastructure, but they have to pay for what they consume. The cost of setting up a server, hiring system administrators, and installing all the needed applications are mostly eliminated. Furthermore, cloud providers can alert their customers if they exceeded certain amount of data usage or reach a specified limit of resource usage on their account.

II. INTRUSION DETECTION SYSTEMS IN CLOUD

In the Cloud computing environment, the deployment of already available Intrusion Detection and Prevention Systems (ID/PS) can't achieve the desired level of security and performance since architecture of cloud computing paradigm is different from existing computing methods like Grid computing. The rapidly growing demand of cloud resources by its users urges the need of some efficient mechanism for secure

provisioning of its resources since intruders may compromise the cloud resources and can cause damages to users' data stored there. It has emphasized the need to develop an IDPS that is specifically designed according to the characteristics of cloud rather than deployment of a traditional IDPS. For this, authors recommended the use of four novel concepts namely; autonomic computing, fuzzy theory, ontology, and risk management. Autonomic computing is the on demand, self-management capability of cloud resources. Fuzzy logic works on the basis of degrees between false and truth, or 0 and 1. It is a probabilistic approach to reach a conclusion instead of using exact values [4].

Intrusion Detection System (IDS) is a security technology, which can detect, prevent and possibly react to computer attacks. In this past, IDSs have proven to be effective mechanisms in conventional local and wide area networks. In a typical network scenario, an IDS generates alerts regarding security threats and logs them for further analysis. Then, a network administrator can decide to act on the IDS judgment and can prevent the user activities. The concept of IDS was first introduced by Denning (1987) during the year 1987. Since then, IDSs have evolved from standalone hardware's to a piece of software and also to a virtual machine (VM) instance which can run on virtual environments like the clouds. Typically, many organizations which use cloud networks require an automated process to monitor various events occurring on their network assets [5].

Therefore, IDS can provide the needed protection against external intruders and internal users who are taking advantage of their privileged accounts. Accordingly, the incorporation of IDS in any network is vital. The location of the IDS is an important factor for achieving efficient event monitoring. In a typical network layout, the IDS can be placed along with other essential security software's like the access control module and antivirus software just behind the corporate firewall. A major distinction between the IDS and a firewall is that the former will continuously monitor the internal part of the network and protects it from internal and external threats. On the other hand, firewalls act like a conditional barrier that only allow defined services, ports or IP addresses to pass through them. Therefore, an intruder can bypass the firewall and can attack the network and databases. In such a scenario, it is hard to stop or recognize the origin of the attack [4, 5].

A. IDS components

There are four main components that all IDSs share regardless of their nature: the sensors, the database, the database manager and the Knowledge Base (KB). Initially, IDS sensors collect data traffic in the network and store them into the cloud database. Next, the cloud database manager invokes the classification system to separate the normal users from intruders. In such systems, the rules stored in the knowledge base are fired by the database manager in coordination with a rule manager to perform inference. Based on the inference, the users are provided with some trust values which are increased periodically for normal users upto the time they get hundred percent reputation. Similarly, the trust score is reduced for malicious users periodically and is stopped and marked as intruder when their trust score becomes less than 50%. On detecting an attack, the database manager informs the security administrator with detailed information about the nature of the event or responds to the incident according to a predefined action plan [5].

B. IDS Classifications

In general, IDSs are classified into different types based on their method of collecting data, their method of analyzing alerts, and their reaction to security threats. According to the method they collect data, IDSs can be Host based (HIDS) or Network based (NIDS). A HIDS usually observes a specific host by installing an agent inside the monitored system and examines its system calls, operating system log and application generated events. This type of tightly coupled model monitors the hosts effectively. Such systems have the advantage of examining system level threats like buffer overflow attacks [6].

C. IDS in the Cloud

In the Cloud Computing environment, an IDS is an important component for security. Cloud consumers always just depend on the cloud provider's security infrastructure. They may need to monitor and protect their virtual existence by implementing IDS with other network security technologies like firewalls, access controls and data encryption within the cloud system. Consequently, cloud clients need to be able to deploy detection systems within their virtual boundaries. The IDS is expected to monitor multiple virtual machines based on the application requirements. The cloud clients should have the control of their management. Cloud based IDS must be able to incorporate IDS rules. These customized rules are written by a security administrator based on the application requirements. Cloud consumers should have the ability to scale the protection coverage of their applications based on the amount and the location of the data being analyzed [7].

III. INTELLIGENT CLASSIFICATION ALGORITHMS

The algorithm called Naïve Bayesian and Intelligent Agent Based Support Vector Machines integrates Naïve Bayesian classification algorithm with Support Vector Machines using intelligent agents for enhancing the classification accuracy.

A. Naïve Bayes Classifiers

Naïve Bayes (NB) classifier uses conditional probability for effective decision making. However, the proposed agent based classification algorithm relaxes the conditional probability. This flexibility reduces the time complexity of the Bayesian classification (Tom Mitchell Algorithm). To explain the proposed NBIASVM, the variables considered in Naïve Baye's classifier are explained here. Given random variables X,Y and Z, we say X is said to be conditionally independent of Y given Z, if and only if the probability distribution governing X is independent of the value of Y given Z; that is

(i, j, k)P(X = xi |Y = yj ,Z = zk) = P(X = xi |Z = zk)

The Naive Bayes algorithm is a classification algorithm which is based on Bayes theorem. This theorem assumes that the given attributes X1 ...Xn are all conditionally independent of one another, given Y. This assumption simplifies the representation of P(X|Y), and also its estimation from the training data [8].

B. Intelligent Agents

Intelligent agents are software programs which are capable of perceiving the environment using sensors, learn the rules governing change and act flexibly using rules. Using these algorithms, the cloud data set is classified into masquerades, DoS, TCP and the OTHERS categories of attacks. The DoS contains all specific Denial of Service attacks like smurf, land, neptune, back and teardrop. The others include the PROBE category which contains the attacks including ipsweep, nmap, portsweep and satan. All the other types of attacks and the normal connections are grouped into the OTHERS category [9].

C. Support Vector Machines

The Support Vector Machine approach transforms data into a feature space F that usually has a high dimension. Moreover, SVM generalization depends only on the geometrical characteristics of the training data, but not on the dimensions of the input space. Training with SVM becomes a quadratic optimization problem with bound constraints and one linear equality constraint. [10] had shown how training a SVM for a pattern recognition problem leads to the following quadratic optimization problem given in equations.

The SVM consists of two phases, in a first phase of the SVM, called the training phase, a decision function is inferred from a set of objects. Moreover, it is assumed that the classification is known a-priori for these objects. The objects of the family of interest are termed as the positive objects and the objects which are from outside the family as the negative objects. In the second phase, termed as testing phase, the decision function is applied to make decision on arbitrary objects in order to predict, whether these objects belong to the family under consideration [11, 12].

D. Naïve Bayes and Intelligent Agent Based Support Vector Machine Classifier

The steps of the NBIASVM are as follows.

Step 1: Read the set of selected of features F
Step 2: Read the user data set U
Step 3: Let t. condition P denotes the user who is an insider and has authenticated credentials.
Step 4: Calculate the posterior probability for that U under P.
Step 5: If feature of F satisfy U under P based on Probability > threshold.
Step 5a: Label under Group 1 and go to step 8.
Step 6: Else, add additional feature. Go to step 4.
Step 7: Add to Group 2
Step 8: Choose new value for U by reading next user data
Step 9: Check whether user violate access rules using Intelligent agents
Step 10: If so put in Group 1 else put in Group 2.
Step 11: Apply SVM to perform classification.
Step 12: If result matches with Naïve Bayes and Agent results, then conform. Repeat the steps 8 to 10 until all user are classified.
Step 13: Stop

IV. EXPERIMENTAL RESULTS

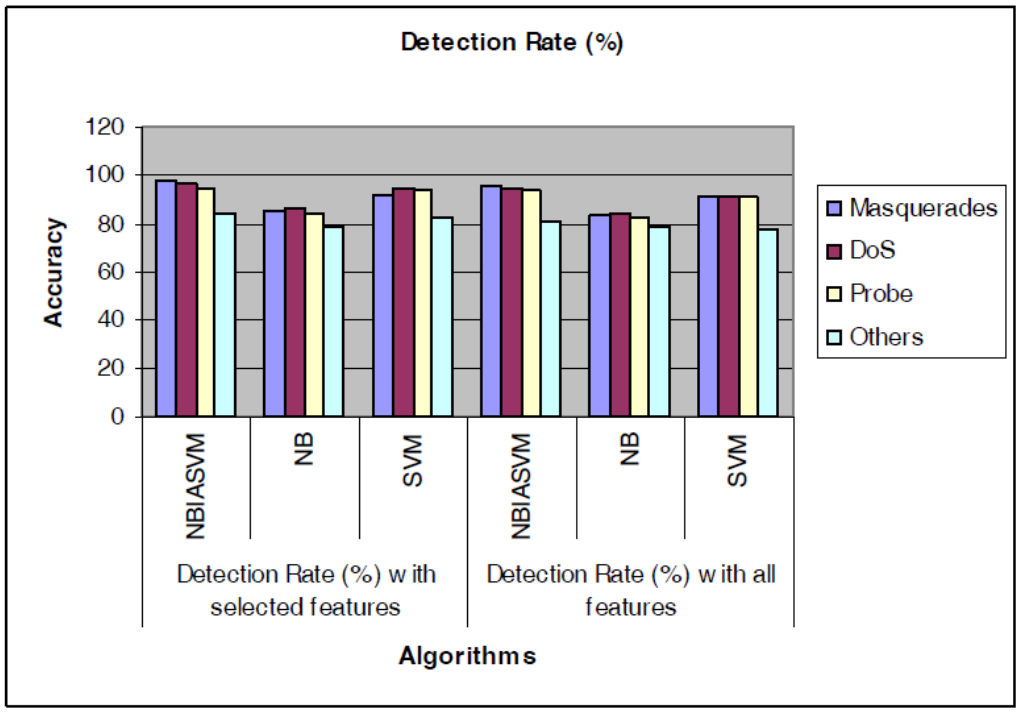
CIDD cloud data set is taken for testing the algorithms with both full features and selected features. Each connection record is described by 29 attributes in the data set. The reduced feature set has 14 features

which selected by using feature selection algorithms in order to use the most contributing features. The experiments are conducted for different set of features with the NBIASVM algorithms. Table shows the comparison between Classification of Attacks Based on the NBIASVM, NB and SVM with Selected Features and with features.

Table I: Detection Rates (%) Comparison between Classification of Attacks Based on the NBIASVM, NB and SVM with Selected Features And with All Features

Attacks	Detection Rate (%) with Selected features			Detection Rate (%) with All features		
	NBIASVM	NB	SVM	NBIASVM	NB	SVM
Masquerades	97.32	85.2	92.3	95.56	83.4	90.52
DoS	96.87	86.3	94.5	95.12	84.72	91.07
Probe	94.53	84.7	93.7	94.03	82.91	90.81
Others	84.64	78.5	82.8	80.74	78.84	78.23

From this table, it can be observed that the intrusion detection rate is improved NBIVSVM with selected features when it is compared with selecting all features for the same classifier. The Chart shows the diagrammatic representation of above Table.



V. CONCLUSIONS

In this research work, a classification algorithms NBIASVM is discussed. The main advantage of this algorithm is that it increases the detection accuracy. It provides better classification accuracy and reduced false positive alarm rate than the existing intrusion detection systems by the use of agents in the intrusion detection and prevention processes.

VI. FUTURE SCOPE

A number of future enhancements are possible to enhance the security of the cloud system further. Future works could be done by this direction by the introduction of temporal features into the intrusion detection system for effective real time feature analysis. This work can also be extended by proposing a new distributed key generation scheme to prevent all types of attacks. Moreover, it is possible to use different types of intelligent and mobile agents to improve the power of distributed processing.

REFERENCES

[1]. Yasir Mehmood, Muhammad Awais Shibli, Umme Habiba, Rahat Masood, "Intrusion Detection System in Cloud Computing: Challenges and opportunities", in 2nd National Conference on Information Assurance (NCIA), December 2013.

[2]. Uttam Kumar and Bhavesh N. Gohil, "A Survey on Intrusion Detection Systems for Cloud Computing Environment", in International Journal of Computer Applications, vol. 109 – No. 1, pp. 6-15, January 2015.

[3]. D. P. Kale and V. M. Thakare, "Different Security Features and Solutions In the Cloud Data Services", ICICV2020, unpublished.

[4]. A. Patel, M. Taghavi, K. Bakhtiyari, J. C. Junior, "An Intrusion Detection and Prevention System in Cloud Computing: A Systematic Overview", Journal of Network and Computer Applications, pp. 25–41, 2013.

[5]. Sindhu, SSS, Geetha, S & Kannan, "Decision tree based light weight intrusion detection using a wrapper approach", Expert Systems with Applications, vol. 39, no.1, pp. 129–141, 2012.

[6]. Denning, DE, "An intrusion detection model", IEEE Transaction on Software Engineering, vol.13, pp. 222-232, 1987.

[7]. Rajeswari, LP & Kannan, 'An active rule approach for network intrusion detection with enhanced C4.5 algorithm', International Journal of Communications, Network and System Sciences, vol. 1, no. 4, pp.285-385, 2008.

[8]. Dewan, M, Farid, Zhang, Chowdhury, Mofizur, Rahman, Hossain, Rebecca, MA & Strachan 2014, "Hybrid decision tree and naive Bayes classifiers for multi-class classification tasks", Expert Systems with Applications, vol.41, pp. 1937–1946, 2008.

[9]. Zubair, Baig, A, Sadiq, Sait, M, Abdul, Rahman & Shaheen, "GMDH-Based networks for intelligent intrusion detection", Engineering Applications of Artificial Intelligence, vol. 26, pp. 1731–1740, 2013.

[10]. Latifur, Khan, Mamoun, Awad, Bhavani & Thuraisingham, "A new intrusion detection system using support vector machines and hierarchical clustering", The VLDB Journal - The International Journal on Very Large Data Bases, Springer-Verlag, New York, vol. 16, no. 4, pp.507-521, 2007.

[11]. Reda, M, Elbasiony, Elsayed, Sallam, A, Tarek, E, Eltobely, Mahmoud M & Fahmy, "A hybrid network intrusion detection framework based on random forests and weighted k-means", Ain Shams Engineering Journal, vol.4, no.4, pp. 753–762, 2013.

[12]. Seyed, Reza, Hasani, Zulaiha, Ali, Othman, Seyed, Mostafa, Mousavi & Kahaki, "Hybrid feature selection algorithm for intrusion detection system", Journal of Computer Science, vol.10, no.6, pp. 1015-1025, 2014.

Dr. Devendra P. Kale "A novel approach to design the intelligent technique for intrusion detection in cloud". *IOSR Journal of Engineering (IOSRJEN)*, 10(1), 2020, pp. 40-44.