International Journal of Interdisciplinary Innovative Research &Development (IJIIRD)
ISSN: 2456-236X
Vol. **05** Special Issue **01** | **2020**

An Implementation of Security Attacks Detection in Cloud using Machine Learning Algorithms

Monika V. Nanane[1], Ankit R. Mune[2], Mrunal G. Khandade[3], Samiksha D. Aghadate[4], Aniruddha B. Hirapure[5]

[1,3,4,5]*B.E. Student, Department of Computer Science & Engineering, PRMITR, Badnera, Amravati, Maharashtra, India*
[2]*Assistant Professor, Department of Computer Science & Engineering, PRMITR, Badnera, Amravati, Maharashtra, India*

ABSTRACT

Cloud computing is an rapidly growing technology which provides reliable and scalable on-demand resources and different services to users with less infrastructures cost. Even though the cloud has lots many advantages, it faces many drawbacks like vulnerability to attacks, network connectivity dependency, downtime, vendor lock-in, limited control. From the above-mentioned drawbacks, a security attack is the main drawback in the cloud. There are many security attacks like Denial-of-service (DOS) attack, SQL injection attack, Side channel attack, Man-in-the-middle attack, Authentication attack. To detect this attack in the cloud the machine learning algorithm like Support vector machine (SVM), Naive Bayes, Decision tree, Logistic regression, Ensemble methods can be used. We will mainly focusing on various security known and unknown attacks in the cloud such as Authentication attack, SQL injection attack and Denial of service attack. And the machine learning algorithms such as Support vector machine is used for detecting these attacks.

Keyword:- Security attacks, Machine learning algorithms, Detection.

1. INTRODUCTION

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 in general used to delineate data centers available to many end users over the Internet. Large clouds, predominant today, frequently have functions distributed over numerous locations from central servers. If the connection to the user is fairly close, it may be designated an edge server. Clouds may be limited to an organization, or be available to many organizations (public cloud). Cloud computing relies on sharing of resources to achieve coherence and economies of scale. Advocates of public and hybrid clouds note that cloud computing allows companies to avoid or minimize beforehand IT infrastructure costs. Supporters also asserts that cloud computing permits pursuits to get their applications up and running faster, with improved manageability and less maintenance, and that it enables IT teams to more rapidly adjust resources to meet fluctuating and unpredictable demand, providing the burst computing capability: high computing power at certain periods of peak demand. Cloud computing is latest trend in IT world. It is Internet-based computing, whereby shared resources, software and information, are provided to computers and other devices on- demand, like the electric grid. This technology has the capacity to admittance a common collection of resources on request. It is proving extremely striking to cash strapped IT departments that are wanted to deliver better services under pressure. The Software as a service (SAAS), Platform as a service (PAAS) and the Infrastructure as a service (IAAS) all together encapsulate to form the cloud. All the above services are the three types of services that is been provided by cloud computing. The problem of attack detection using machine-learning techniques is not new to literature. While signature detection techniques can detect attacks based on signatures of already learnt attacks, anomaly detection techniques learn network traffic from a baseline profile and detect anomalies as ones that deviate significantly from the baseline profile. Signature detection techniques are effective against known attacks while anomaly detection has the ability to detect unknown and new attacks (zero-day).

1.1 Motivation

Cloud security is the protection of data stored online from theft, leakage, and deletion. The cloud encounters many security attacks due to its disadvantages. The various cloud attacks like Denial of service attack, SQL injection attack, Man in the middle attack and the authentication attack are discussed below. The attacks may happen at different parts of the cloud like the data storage, during a transaction, during resource utilization and sharing. The loss of the attack can be lower to higher based on the type of attack. The reason for the attack in the cloud is due to the huge

increase in the use of cloud services. Multiple approaches are required to counter each of such attacks.

2. RELATED WORK

- Assume that a cloud provider trained a Support Vector Machine (SVM) classifier on some of the features of the VMs under a certain infrastructure. These features include CPU, network, memory and I/O load. Assume now that the cloud provider, due to some business factors, decides to adjust some of the resources of the VMs. This adjustment includes revoking 45% from some of the resources of the VMs. Such an adjustment will result in as significant decrease in the DoS detection accuracy rate [3].
- Evolution of Denial of Service (DoS) attacks to Distributed DoS (DDoS) attacks . Cloud Security Alliance has identified DDoS attack as one of the nine major threats. A detailed survey of other possible threats in cloud environment and intrusion detection techniques is given. A hybrid approach of decision trees and SVM has been proposed. The authors propose Bayesian network based model to detect the network threats. Data mining approaches have been proved efficient for anomaly detection in networks[5].
- The brute force attack has been and still is, one of the most prevalent attacks on the Internet. In this paper we investigate the use of machine learning methods to detect brute force attacks at the network level by using flow data. To this end we collected real word data which was labeled by network experts. Using the labeled data, we trained 4 different classifiers and evaluated their results based on average AUC values obtained across 4 runs of 5-fold cross-validation. Our results show that with the application of machine learning methods, we can achieve very good prediction results in detecting SSH brute force attacks[7]. Brute force attacks are one of the most prevalent types of attacks in computer networks [8], [9]. In a brute force attack on the SSH protocol the attacker tries to log in to a user's account, and continues trying different passwords on the victim's machine to reveal the login password.
- SQL injection attack is a very serious problem of web applications. Finding the efficient solution of this problem is essential. Researchers have developed many techniques to detect and prevent this vulnerability. There is no appropriate solution that can prevent all types of SQL injection attacks. SQL Injection attacks remain to be one of top concerns for cyber security researchers. Signature based SQL Injection detection methods are no longer reliable as attackers are using new types of SQL Injections each time[12]. There is a need for SQL Injection detection mechanisms that are capable of identifying new, never before seen attacks. Applying machine learning to the field of cyber-security is being considered by many researchers. Since machine learning in cyber-security is still a developing research area, there are not many libraries and open source tools that are machine learning specific and apply to problems related to threats and attacks[10], [11].
- Two machine learning classification algorithms are implemented on the problem, which are, Na¨ıve Bayes Classifier and Gradient Boosting Classifier. Na¨ıve Bayes classifier machine learning model provides results with an accuracy of 92.8%.Ensemble learning methods are said to provide results with better accuracy as they implement multiple simple classifiers to improve error and accuracy. Hence Gradient Boosting Classifier from ensemble learning is selected to be implemented on the SQL Injection classification problem [12], [13].

3. SYSTEM ANALYSIS, DESIGN AND IMPLEMENTATION

3.1 Analysis

3.1.1 Problem Definition

Attacks are broadly classified into two types viz. Known attacks and Unknown attacks.

1) Known Attacks : Known attacks are the attack for where the methods of attack are already known and system is designed to detect it. The example of such attack is "Authentication Attack" where brute force or dictionary attack methods are used. Such attacks can be directly detected by the system.
2) Unknown Attacks: Unknown attack are the attacks for which the patterns or method cannot be determined. Machine learning is then used to detect such attacks. An example of such attack is Denial of Service (DoS) attack. The model is trained based on the dataset. The model then classify the requests into attack or normal requests.

3.1.2 Objective

- To prevent SQL based known attacks such SQL Injection.
- To prevent authentication based attacks such as brute force.
- To train and deploy SVM model.
- To prevent DDOS attacks using SVM model.

3.1 Design

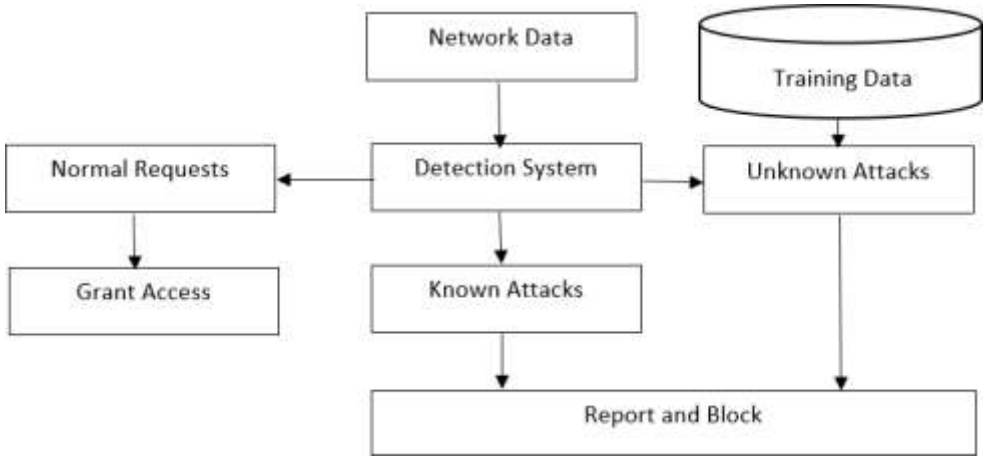

Fig-1 Block diagram of proposed system

➢ Proposed System

The security attack detection system consists of two modules know attack detection and unknown attack detection. Attacks like authentication attack or sql injection can be detected using checks. For unknown patterns of attack like Denial of Service, machine learning is used.

- Dataset: Dataset contains network records and labels saying if the network request is normal or attack.
- Pre-Processing: Dataset is pre-processed and cleaned of missing and faulty records for better accuracy in model generation.
- SVM Training: SVM algorithm is applied on the dataset and a model is generated. The algorithm runs several iteration refining the model for better accuracy.
- Model Deployment: The trained model is deployed on the system for intrusion detection.
- Request Interception: The network request are intercepted and processed first by intrusion detection system. First the request is checked for known attacks and if the attack is detected then the request is blocked and reported.
- SVM Attack Prediction: If the known attack check is passed, then the request is sent through the SVM model. The model then predicts if the request is normal or part of an attack. If attack is predicted by the model then the request is blocked and reported.
- Attack Report**:** All the detected attacks are reported and logged.

3.2 Implementation

- SQL Injection Detection: SQL Injection is detected when during the login process by processing and sanitizing the input requests.
- Authentication attack: Authentication attack like brute force attack are stopped by checking the number of failed login and then blocking the account after certain number of attempts.
- DDOS Attack: SVM model is trained over a dataset for detecting malicious attacks. The model is trained to differentiate between malicious packets and normal packets. This model is deployed to filter the network packets and block malicious packets.
- Admin: Admin can train and deploy SVM models. All detected attacks are reported to admin. Admin can block or unblock user accounts.
- User: User can login and store files on the cloud. User can upload and download the files

3.3.1 System Execution Detail

- User Module : The user module consist of four sections: home, upload, profile and change password. Home section has login window. Here in above Fig-2 upload section is shown where user can upload files in any format along with the file name or document title and the document uploaded date and time

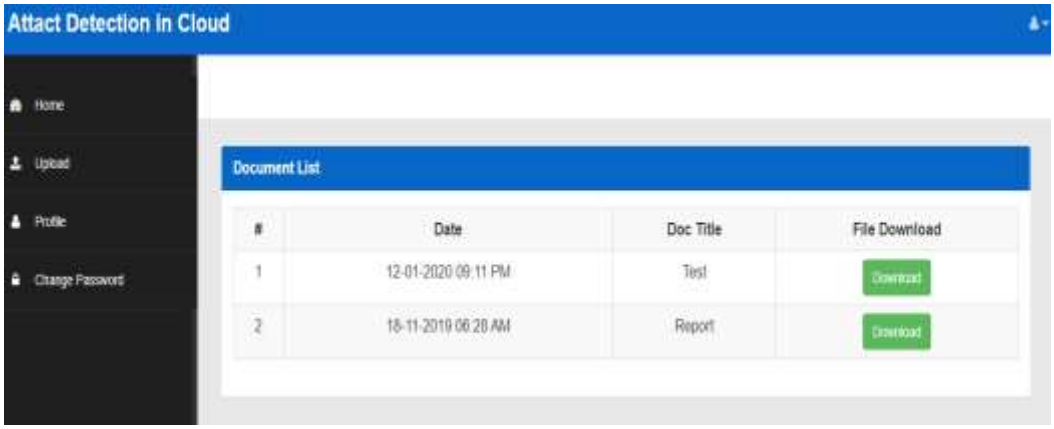

Fig-2 User module

- SQL Injection Detection: The below Fig-3 shows how SQL injection attacks realize and how it is detected by the system. SQL injections utilize weakness of a system to misguide the application into running a database backend query or command. The query will return all rows in the table, which is not the original intention. SQL injection attacks can be mitigated by ensuring proper application design, especially in modules that require user input to run database queries or commands. Fig-3 (a) shows that the attacker enter the SQL query for accessing the information and (b) shows how the SQL attack detected by the system.

Fig-3 SQL injection attack: (a) how it occurs (b) attack detection

- Authentication attack: A Brute Force Attack is the simplest method to gain access to a site or server (or anything that is password protected). It tries various combinations of usernames and passwords again and again until it gets in. Usually, every common ID (for e.g. “admin”) has a password. All you need to do is try to guess the password. Let’s say if it’s a 2-digit-pin, you have 10 numeric digits from 0 to 9. It means there are 100 possibilities. In Fig-4 (a) shows the first attempt we can try only for three attempts. If user tries the combination of id and password for more than 3 attempts then the id will get blocked as shown in (b).

Fig-4 Authentication attack: (a) how it occurs (b) attack detection

- Admin Attack List: The below Fig-5 shows the admin module consist of four sections: home, user list, prepare dataset, and train model. On the home page attack list is shown, which attack is detected along with the attack occurred date and time and system's IP address. For known attack methods like SQL injection and brute force attack, attack name is displayed along with the system's IP address. And for unknown attack like DDOS attack, attack name is displayed in the table with the blocked requests. In this attack IP address will not shown because such attack occurs in the network as per the request and the dataset used.

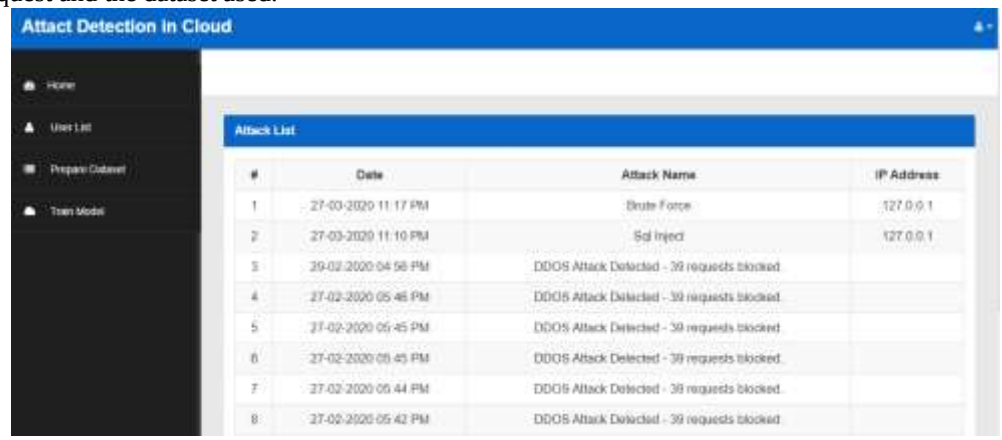

Fig-5 Admin module to show attack detection list

- SVM Model Training: In below Fig-6 prepare dataset is trained by support vector machine model. Prepare dataset is already stored in the database in the form of table which then converted into sparse matrix. Here we use the two classes normal and anomaly class, normal class is represented in numeric format as 1 and anomaly as -1. Each string value in the dataset is converted into number as 1 to 84. Data packets are send to SVM model to check whether the request is from normal user or from intruder. SVM training result consist of prepare dataset, its prediction and actual result. By comparing actual value and predicted value, status is shown whether it is correct or not and on the basis of status total accuracy is calculated. It varies each time the model is trained depending on the packets sent by the network.

Fig-6 SVM Training Model

- DDoS Attack: Fig-7 shows the attack detection report where the following parameters like total request count, attack requests, attack detected, and compared status of correct and incorrect request is given. In prediction, anamoly is highlighted by red color and normal packets by green color. Based on correct and incorrect status accurate percentage is calculated.

Fig-7 DDoS attack detection

4. CONCLUSIONS

Cloud security has become important as more people are using it every day. There are various types of attacks targeted at cloud environment. We have implemented a system which detects and reports SQL Injection attack, Authentication attack and DDOS attacks. For SQL Injection attack, inputs are processed and sensitized for any malicious SQL contents. For authentication brute force attack, users are blocked after a certain number unsuccessful login attempts. For detecting DDOS attacks, a SVM model is trained and deployed to differentiate between normal data and malicious data. SVM model is trained over a dataset and deployed. This model then detects malicious data and blocks it.

5. ACKNOWLEDGEMENT

We express our sincere gratitude to Dr. G. R. Bamnote, Head Department of CSE, for his valuable guidance and advice. Also we would like to thanks to our guide Prof. A .R. Mune and the faculty members for their continuous support and encouragement.

6. REFERENCES

[1]. Dhivya R, Dharshana R, Divya V: Security Attacks Detection in Cloud using Machine Learning Algorithms.
[2]. MarwaneZekri, Said El Kafhali, Noureddine Aboutabit, and Youssef Saadi: DDoS Attack Detection using Machine Learning Techniques in Cloud Computing Environments.
[3]. Adel Abusitta, Martine Bellaiche, and Michel Dagenai: An SVM-based framework for detecting DoS attacks in virtualized clouds under changing environment, Journal of Cloud Computing: Advances, Systems, and Applications Abusittaetal. Journal of Cloud Computing: Advances, Systems.
[4]. Zainab S. Alwan, Manal F. Younis, Detection and Prevention of SQL Injection Attack: A Survey, International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 6, Issue. 8, August 2017.
[5]. Deval Bhamare, Tara Salman, Mohhamed Samaka, Aiman Erbad, Raj Jain: Feasibility of Supervised Machine Learning for Cloud Security.(2016)
[6]. Shubham Jawanjal, Shubham Shegokar, Vandana Nandurkar, Radhika Ardak, Sneha Chaudhari, Snehal Rithe, Prof.Sneha R. Sontake: An Efficient Technique for Detection and Prevention of SQL Injection Attack in Cloud.(2018)
[7]. Maryam M Najafabadi, Taghi Khoshgoftaar, Clifford Kemp, Naeem Seliya: “Machine Learning for Detecting Brute Force Attacks at Network Level.” (Nov 2014)
[8]. E. Alata, V. Nicomette, M. Kaaniche, M. Dacier, "Lessons Learned from the Deployment of a High interaction Honeypot," in Dependable Computing Conference, 2006. EDCC '06. Sixth European, Coimbra, 2006.
[9]."Hewlett-Packard Development Company. Top Cyber Security Risks Threat Report for," 2010.
[10].Sonali Mishra, “SQL Injection Detection using Machine Learning”, from https: //scholarworks.sjsu.edu/cgi/viewcontent.cgi?article=1727context=etdprojects, on 23 May 2019 pp.10 - 29.
[11]. J. Abirami, R. Devakunchari and C. Valliyammai, "A top web security vulnerability SQL injection attack - Survey," 2015 Seventh International Conference on Advanced Computing (ICoAC), Chennai, 2015, pp. 1-9.
[12]. Tareek Pattewa, Hitesh Patil, Harshada Patil, Neha Patil, MuskanTaneja ,Tushar Wadile: Detection of SQL Injection using Machine Learning: A Survey. (11 Nov 2019)
[13]. Bojken Shehu and Aleksander Xhuvani ,”A Literature Review and Comparative Analyses on SQL Injection: Vulnerabilities, Attacks and their Prevention and Detection Techniques” from https ://pdfs.semanticscholar.org,Vol.11,Issue4,No 1,July 2014 pp 20 – 34.