International Engineering Journal For Research & Development

Vol.4
Issue - 7

E-ISSN NO:-2349-0721

Impact factor : 6.03

SECURITY ATTACKS DETECTION IN CLOUD USING MACHINE LEARNING ALGORITHMS :A SURVEY

Monika V. Nanane
B.E. Student, *Department of Computer Science & Engineering*
PRMITR, Badnera
Amravati, India
monikananane123@gmail.com

Ankit R. Mune
Assistant Professor, *Department of Computer Science & Engineering*
PRMITR, Badnera
Amravati, India
armune@mitra.ac.in

Mrunal G. Khandade
B.E. Student, *Department of Computer Science & Engineering*
PRMITR, Badnera
Amravati, India
mrunalikhan98@gmail.com

Abstract—

Cloud computing is an evolving technology that provides reliable and scalable on-demand resources and different services to users with fewer infrastructures cost. Even though the cloud has many advantages it faces many drawbacks like vulnerability to attacks, network connectivity dependency, downtime, vendor lock-in, limited control. From the above-mentioned disadvantages, a security attack is the main drawback in the cloud. There are various 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.

Keywords— Security attacks, Machine learning algorithms, Detection.

Introduction

The cloud is a booming technology in the computer sector. It is present at the remote location and it's providing services over the network. The user can be configured, accessing and manipulating the application such as data storage, infrastructure, server and application. The user can access anything as services such as infrastructure, platform, and software anywhere in the world from the cloud through the internet.But oneof the disadvantages in cloud computing is security attacks. This drawback is due to the data storage at different geographical areas in cloud computing.

The below fig.1 describes the various security threats in public clouds as per the cloud security report provide by cloud security insiders, thus from the chart the misconfiguration of the cloud platform is about 62%, unauthorized access is about 55%, Insecure interfaces /APIs is about 50%, Hijacking of accounts, services or traffic is about 47%.

Nowadays, these security attack attempts have been increasing and DoS (Denial of Service) attacks are one of the major threat in computer networks. It attempts server's resources unavailable and generates massive traffic on the network. These attacks are evolving very quickly in scope and complexity.

Fig.1. Security threats in public cloud

ATTACKS ON CLOUD

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 and "Sql Injection". Such attacks can be directly detected by the system.

1.1 *SQL Injection Attack* : An SQL injection attack is an attempt to issue SQL commands to a database via a website interface. This is to gain stored database information, including usernames and passwords. This code injection technique exploits security vulnerabilities in an application's database layer. Hackers exploit poorly coded websites and web apps to inject SQL commands, for example, taking advantage of a login form to gain access to the data stored in the database. In simple terms, SQL injection attacks occur because the user-input fields permit the SQL statements to pass through and directly query the database.

Fig.2. SQL Injection Attack

1.2 *AuthenticationAttack* :The Authentication attack mainly focuses on the authentication part of the cloud services. The primary authentication in most of the services is the username and the password which is a type of the knowledge-based authentication. The secondary authentication like shared secret questions, site keys, virtual keyboards is used by secure functioning organizations like the financial company. Some of the authentication attacks are the Brute Force Attacks, Dictionary Attack, Shoulder Surfing, Replay Attacks, Phishing Attacks, Key Loggers.

- Brute force attack: This attack is like a trial and error method; this attack is launched by guessing passwords containing all possible combinations of letters, numbers and alphanumeric characters until the attacker get the correct password. Brute forceattackusually carried out using automated methodsdemands a lot of computing power and time to be successful.

- Dictionary attack: Here the attacker tries to guess a password from a pre-computed dictionary of passwords.To resist this type of an attack, the password should be random and should not be a

dictionary word. Even passwords in mother tongues are not secure as attackershave dictionaries of most of the regional languages

- .Keyloggers: It is a form of a software program, where it monitors the actions of the user by recording each and every key pressed by the user.
- Phishing attack : In this attack, the attacker redirects the user to the fake websites to get the passwords and the pin codes of the user, it is a kind of the web-based attack.

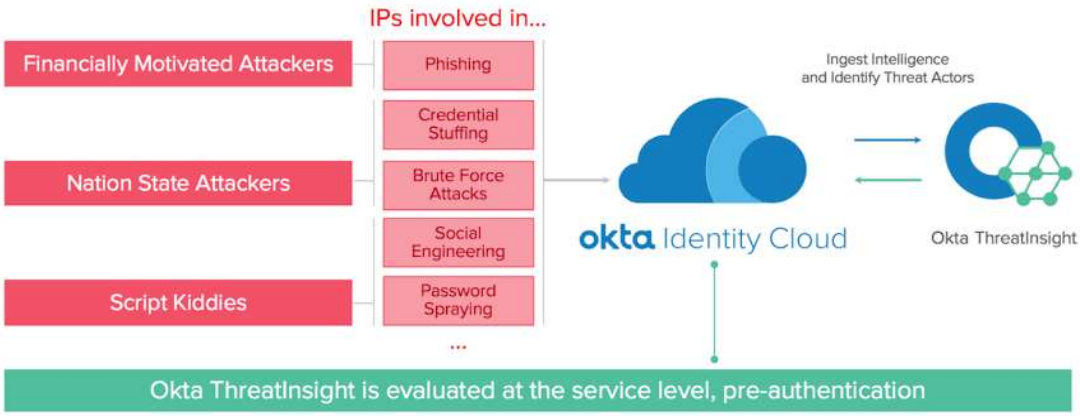

Fig.3. Authentication Attack

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.

2.1 *Denial of Service Attack :*Denial of service attack the targeted cloud system is overloaded with the service requests from the attacker that stops it from responding to the upcoming new requests and to its users. According to some of the cloud security alliance, this cloud is very much vulnerable to this Dos attack. The Denial of service attack can be categorized into the DoS attack and the DDoS (Distributed denial of service attack). The attack was done using the single system and the single network is known as the DoS attack. The attack was done using multiple systems and the multiple networks are known as the Distributed denial of service attack (DDoS).

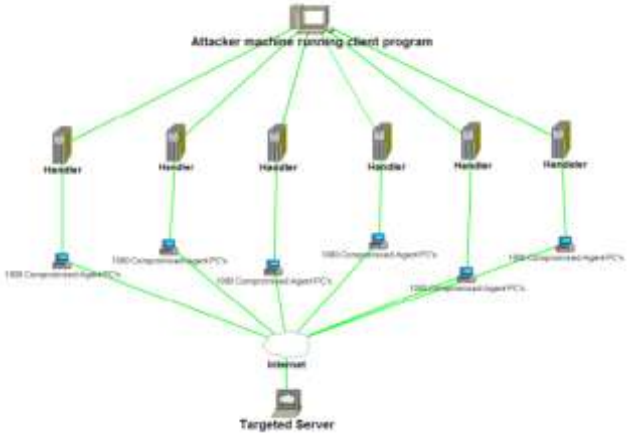

Fig.4. Denial of service attack

A MACHINE LEARNINGALGORITHM FOR DETECTION

The machine learning algorithm allows software applications to produce accurate predicting outcomes without being explicitly programmed. The machine learning algorithm can be divided into classification

algorithms and clustering algorithms. Some of the classification algorithms are the Naïve Bayes, support vector machine (SVM), decision tree, logistic regression, and ensemble methods. In this paper, we are going to use the classification algorithm.

1. Support Vector Machine (SVM) : SVM is used in classification and regression. classification can be viewed as the task of separating classes in feature space. It became famous when using the image as input, it gave good accuracy. Currently, SVM used in object detection and recognition, content-based image retrieval, text recognition, biometrics, speech recognition etc. SVM is a practical learning method based on statistical learning theory. Construct a hyperplane in the decision surface in such a way that the margin of separation between positive and negative. The goal of SVM is to find the particular hyperplane of which the margin is maximized. The particular data point for which the first or second line of the equation is satisfied with the equality sign is called a support vector.

   The objective of the support vector machine algorithm is to find a hyperplane in an N-dimensional space(N-the number of features) that distinctly classifies the data points.

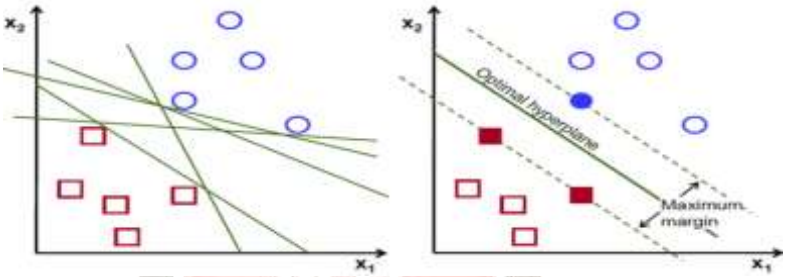

Fig.5. Possible hyperplanes

To separate the two classes of data points, there are many possible hyperplanes that could be chosen. Our objective is to find a plane that has the maximum margin, i.e the maximum distance between data points of both classes. Maximizing the margin distance provides some reinforcement so that future data points can be classified with more confidence.

- Hyperplanes:Hyperplanes are decision boundaries that help classify the data points. Data points falling on either side of the hyperplane can be attributed to different classes. Also, the dimension of the hyperplane depends upon the number of features. If the number of input features is 2, then the hyperplane is just a line. If the number of input features is 3, then the hyperplane becomes a two-dimensional plane.

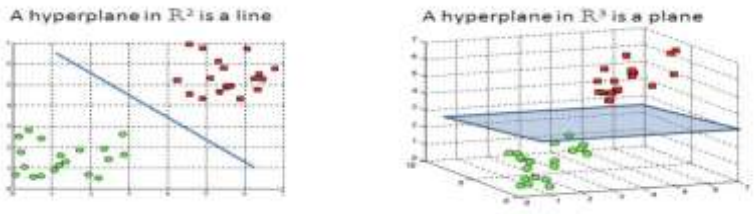

Fig.6. Hyperplanes in 2D and 3D feature space

- Support Vectors: Support vectors are data points that are closer to the hyperplane and influence the position and orientation of the hyperplane. Using these support vectors, we maximize the margin of the classifier. Deleting the support vectors will change the position of the hyperplane. These are the points that help us build our SVM.

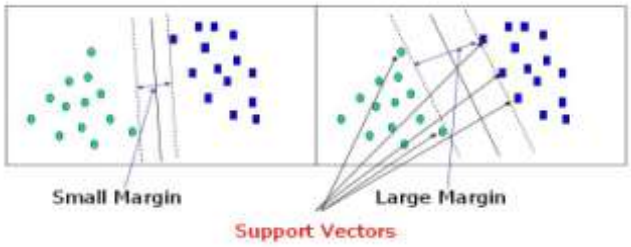

Fig.7. Support vectors

PROBLEM STATEMENT FOR SYSTEM

According to some of the cloud security aliance, this cloud is very much vulnerable to this Dos attack.SQL injection attack the attacker injects the victim system with the malicious service or the malicious virtual machine. Here the attacker creates its own malicious virtual machine or the malicious service module and tries to add it into the cloud system. Then the attacker must behave so as to make the cloud system believe that it is a valid service. If the attacker succeeds then the cloud automatically redirects all the requests to this malicious service. Now the attacker can access the service requests of the victim services.The Authentication attack mainly focuses on the authentication part of the cloud services.

RELATED WORK

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].

PROPOSED APPROACH OF 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.

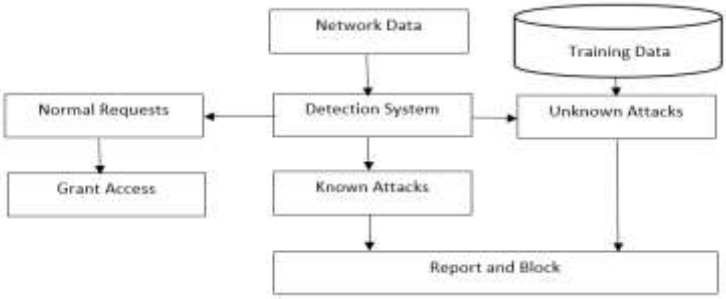

Fig.8. Proposed system

CONCLUSION

The Security attack detection is a very difficult problem in cloud computing.A machine learning algorithm can be used to detect the attack such as support vector machine (SVM). Machine learning algorithms provide with the efficient output.We will work on known and unknown attacks using the machine learning algorithm to enhance the system.

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.

REFERENCES

1. Dhivya R, Dharshana R, Divya V:Security Attacks Detection in Cloud using Machine Learning Algorithms. (2019)
2. MarwaneZekri, Said El Kafhali, NoureddineAboutabit, and Youssef Saadi:DDoS Attack Detection using Machine Learning Techniques in Cloud Computing Environments. (2017)
3. Ankit R. Mune and P. R. Pardhi : Security for cloud computing data using a security cloud as a Third party auditor (TPA): A Survey, International Journal of Advanced Research in Computer and Communication Engineering (Vol. 3, Issue 3, March 2014).
4. Ankit R. Mune and P. R. Pardhi : An Implementation of Security Cloud for Cloud Computing Data as a TPA, International Journal of Engineering Trends and Technology (IJETT) – Volume 12 Number 7 – (Jun 2014)
5. Prof. Ankit R. Mune and Dr .M. B. Chandak : DEFFIE HELLMAN KEY EXCHANGE ALGORITHM FOR SECURE CLOUD COMPUTING DATA,InternationalJoural of Pure and Applied Research in Engineering and Technology(Vol. 3, Issue 9, May 2015).
6. 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. (2018)
7. Zainab S. Alwan, Manal F. Younis, Detection and Prevention of SQL Injection Attack: A Survey, International Journal of Computer Science and Mobile Computing. (Issue. 8, August 2017)
8. DevalBhamare, Tara Salman, MohhamedSamaka, AimanErbad, Raj Jain: Feasibility of Supervised Machine Learning for Cloud Security.(2016)
9. U. Kumar, “A Survey on Intrusion Detection Systems for Cloud Computing Environment,” International Journal of Computer Applications.(2015)
10. Donghoon Kim and Ki Young Lee, “Detection of DDoS Attack on the Client Side Using Support Vector Machine”.(2017)