Intrusion detection and prevention of DDOS and SQL Injection based firewall attacks

Mrs. Revathi.M[1], Jackma Vincelet[2], Janani.R[3], Bavani.E[4]
[1]*Assistant Professor, Department of CSE, Agni College of Technology, Chennai*
[2, 3, 4] *UG Students, Department of CSE, Agni College of Technology, Chennai*

Abstract **- As in recent days, most of the applications host on cloud, Security is a major concern for the data owners. The cloud environment has to be secure and protect data owner data from cloud attacks. In this project work, we study about securing firewall against client-side attacks namely Denial of firewall and SQL injection attacks. Denial of firewall is nothing but overloading the firewall by bursting n number of requests through vulnerable scripts. SQL injection attack is defined as bypassing the security protocols by malicious scripts. Thus, we proposed to design and develop a web application to detect and prevent denial of firewall and SQL injection attacks. The denial of firewall attack can be performed using Java environment-based servers and prevention can be performed using Digital Signature Algorithm (DSA) to detect the malicious script-based requests. In our application, various types of SQL injection attacks namely SQL login bypass, Blind injection, SQL sleep attack, Data fetching attack are analysed and performed. The SQL injection attack can be prevented using PREPARE statements. These statements are created to make the SQL queries more efficient and render security benefits. This statement provides an effective prevention mechanism against SQL injection attacks. Thus, validation and processing of the user queries is an important role for eliminating malicious queries performed by intruders. Thus, our proposed solution, provides high security against firewall attacks namely denial of firewall and SQL injection securing the data owner files and preventing compromising of firewall.**

Index Terms **- Network Security, Distributed Denial of Service, SQL injection Attack, Digital Signature Algorithm, RSA Algorithm, PREPARE Statements.**

I.INTRODUCTION

Cloud computing demand and usage has been significantly increasing nowadays. To access the data from a cloud server, the internet is needed, thus providing provision of a centralized server to connect the devices and obtain the input data from anywhere. Cloud computing provides various advantages to the end users such as flexibility, accessibility, availability. Cloud is popular for storing the data owner data and provides access of data from anywhere. Thus, advantage also leads to serious challenges such as because of the centralized server-based approach this always invokes the risk of attack. As few online articles state that 26 frequent cloud attacks are under existence and have been used for obtaining the data owner data, information without un authorization. These cloud attacks play a vital role with regard to the security aspect. Usually, the cloud attacks are defined in two types such as active and passive attacks. Passive attacks are defined as intruders trying to access the data while data traveling in the network such as port scanner, wiretapping etc. Active attacks are intruders performing malicious activities to disturb the normal operational process such as IP Spoofing, phishing, DDOS, SQL injections, malware injection etc.

Distributed Denial of Service (DDOS) is one of the serious attack which is frequent now a days. This can be initiated by the distributed system or generated from a single host. Sudden bursts of requests would hold the server in processing the requests and response. DDOS attack also extracts all the resources. The main challenge is validation of the incoming packets to be valid and generated from the legal source. DDOS attack is a dangerous attack on internet now a days. This is performed by hackers, bots and auto malicious scripts targeting a node making the node unavailable. Now increased hackers and wide spread of bots make DDOS attack incidents more common. In DDOS attack the hackers attacks a single target most which is mostly a server compromising it resulting to stop all its services. DDOS attackers also use to attack individual system by installing malware into victim system without their knowledge.

Also because of the internet, online transactions, information exchange has increased significantly. Thus, all web-based applications have their own database with data owner secret and sensitive information. If the application is not secure, many database-based attacks can be executed. Among this, SQL Injection Attack (SQLIA) is more dangerous which targets the database of the application to steal the user data without authorization. Usually, hackers perform this attack by modifying the SQL query according to the application, if the application fields, forms are not validated efficiently. These different types of SQL injection attacks are SQL login bypass, blind injection, SQL sleep attack and data fetching attack.

Cloud attacks are the major concern for the cloud computing, Internet of Things (IoT) domains. Security, trust are the challenges in cloud-based web applications. Thus, motivated towards security, I have decided to study two frequent vulnerabilities in this project invoking their attack and preventing measures. For the study, I have decided on DDOS and SQL injection attacks. Thus, this automatic detection and prevention measures in the web application would gain data owner confidentiality, trust thus opening business opportunities for the cloud, web service providers.

II.RELATED WORK

Various researchers have proposed solutions for detecting DDoS attacks in wireless IoT environments. We will discuss them in this section and Table I gives an overview of them.

Sharma et al. [1] have proposed the OpCloudSec framework for securing from the DDoS attack. The authors have leveraged the usage of cloud and wireless SDN. They have utilized the deep belief network to detect the attack. If an attack is detected, it notifies the controller else the packet is forwarded normally. A deep belief network is prone to failure when the inputs are ambiguous, as it does not make adjustments to features of a lower level due to a single round of bottom-up pass. IoT is resource constrained and hence subject to noise, thereby no guarantee of unambiguous input at all times from IoT.

Yin et al. [2] have proposed a DDoS attack detection algorithm that runs in the SD-IoT controller. It evaluates the cosine similarity of the Packet_In rate at the input port. When the cosine similarity exceeds a threshold, it is marked as a DDoS attack. Thus, the victim port is found, and the attack packets are dropped. The threshold setting is crucial and a single threshold value may not be sufficient for all the scenarios.

Sicari et al. [3] have proposed the REATO framework that detects the DDoS attack based on various metrics, such as count of connection requests; count of packets; count of invalid packets, such as bad request, unknown data type, and average response time; and CPU and memory usage. This method is also threshold based. A single value will not be suitable due to dynamism in the network.

Mehmood et al. [4] have utilized the Naive Bayes supervised algorithm for detecting attacks. The trained model is deployed in multiple agents that are distributed across the network to detect DDoS. If DDoS is detected, the event is terminated. A supervised ML algorithm is not scalable for a huge IoT network since it is computationally an intensive task to label a huge amount of traffic and also prone to error.

Meidan et al. [5] have utilized the deep autoencoder model deployed in all the IoT to detect if they are infected by malware, such as Mirai, Bashlite, etc. Working of a deep autoencoder depends on an objective function modeled for the scenario. It is an overhead to model the objective function for diverse IoT.

III.EXISTING SYSTEM

We think firewalls are secure but it’s not many vulnerabilities that compromise the firewalls. Hackers /intruders exploit the firewall using malicious scripts and access the server/ applications. There is no deployed technology that has successfully defended against DDOS attacks. Most of the approaches focus, perhaps understandably, on protection of customer sites against incoming attacks. This turns out to be very difficult to do with today's Internet architecture and protocols. Thus, in the existing system, both firewall security for servers and application security are not efficient and highly secure. There are a number of existing tools available, both hardware and software based, to deal with SQL-Injection attacks. Tools exist to detect SQL-Injection attacks while others try to identify and fix SQL-Injection vulnerabilities. The following are a few software ones we will discuss.

- GreenSQL

- dotDefender
- CodeScan Labs: SQL-Injection

Green SQL is a free Open-Source database firewall that sits between the web server and the database server and is used to protect databases from SQL injection attacks. dotDefender is a web application firewall that offers a SQL-Injection solution. dotDefender is a multi-platform solution running on Apache and IIS web servers. SQL-Injection detection product. It has the capability to scan web application source code that you selected for code syntax vulnerabilities. It subsequently generates a "debug style" report.

IV.PROPOSED SYSTEM

In this project, we analyze Distributed Denial of Service (DDoS) attack detection and prevention measures using software defined policies. DDOS is an attack that overloads the firewall by malicious scripts. Our proposed system provides an efficient prevention method named Digital Signature Algorithm (DSA) to prevent DDOS attack.

Our proposed system provides automatic intrusion detection and prevention against DDOS attack. Also our proposed system provides the infrastructure details before and after attacks.

V.ALGORITHM

DDOS prevention measures include identification of anomalies in the received packets. Also due to large availability of the spamming bots demand to develop a secure system to limit the bot-based attack attempts.

1. Obtain the incoming, outgoing packets in the network and also analyse the information flow as per the process.
2. Pre-processing the traffic and predicting the load in the network.
3. Also analyse and obtain the prediction results and errors.
4. We can also use chaos theory-based concepts to predict the abnormal overloading of requests.
5. DDOS attack is detected by training the attacking pattern model based on the historical data.

VI.PROPOSED METHODOLOGY

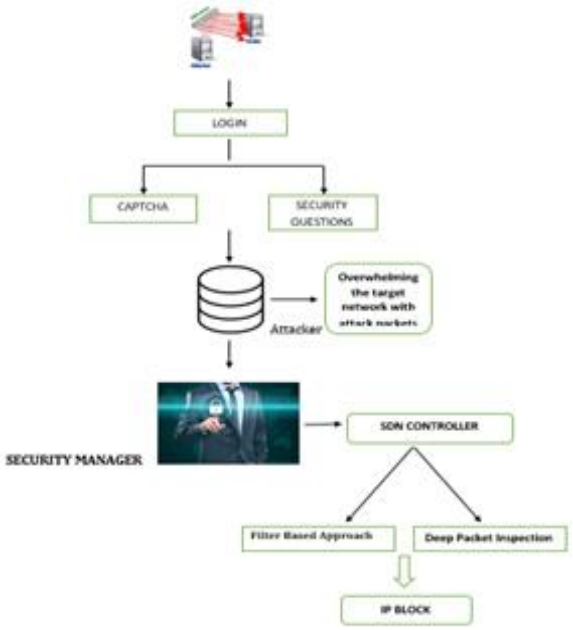

Fig 1. DDOS Attack Methodology

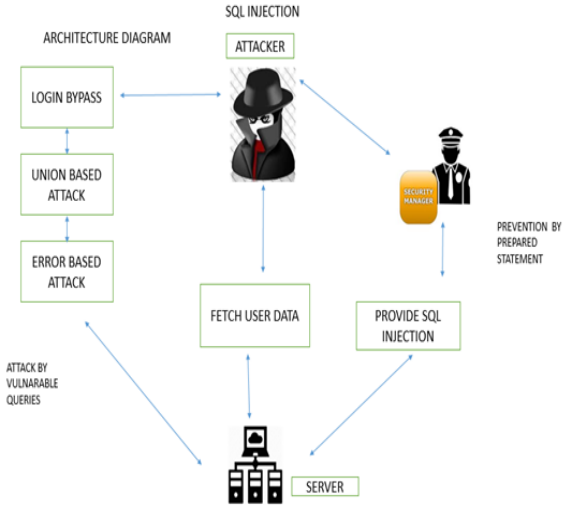

Fig 2. SQL Injection Methodology

Distributed Denial of Service (DDOS) Attack:

This attack is defined as intruders perform this attack in a careful manner to generate the traffic through malicious scripts, several systems to overload the firewall. Distributed based targeting the victim system is performed by the intruder by transmitting dummy packets to all the connected systems to overload the victim server and make it down

SQL Injection Attack:

An successful SQL injection attack can able to inject, modify, delete, update the data owner stored information's on the backend database. SQL injection

is used to read sensitive information's of the data owner from the database without authorization and can able to execute malicious script on the database to shut down the server and stop processing the request.

VII.EXPERIMENTAL RESULTS

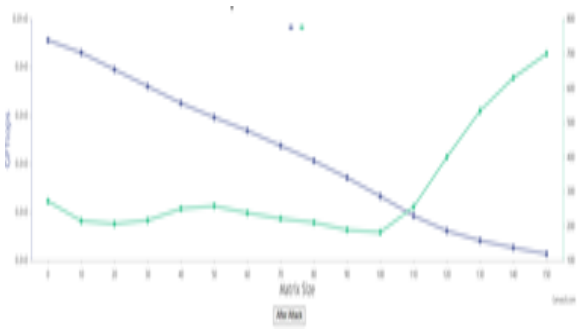

Fig3. CPU performance before attack

The CPU performance for intrusion detection systems is setup at a planned position across the network in order to determine the traffic from other devices on the network. It performs an observation of passing traffic on the whole subnet and matches the traffic that is passed on the subnets to the collection of known attacks.

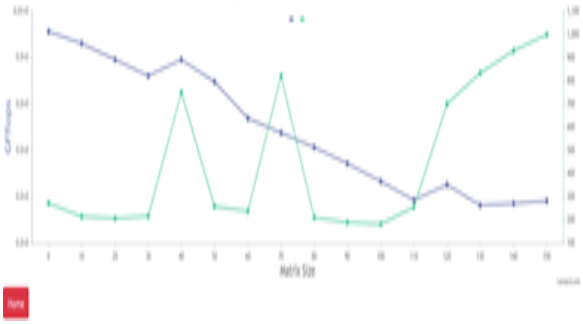

Fig4. CPU performance after attack

The CPU performance after attack is identified in order to see if someone is trying to crack the firewall. Once an attack or an abnormal behavior is observed, and the alert is sent to the administrator to investigate. Firewalls restrict access between networks to prevent intrusion and if an attack is from inside the network will signal outwardly for intrusions to stop them from happening.

VIII.CONCLUSION

The proposed methodology can contribute trust and confidentiality to the data owners in using cloud-based applications. The data stored within the server is protected from DDOS and SQL injection attacks by using automatic prevention policies based on the previous patterns. These patterns are used to train the system to automatically detect and prevent the DDOS and SQL injection attack within a short period time reducing manual based network operator efforts. Thus, this system can be further enhanced with automatic intrusion and detection of 26+ cloud attacks thus motivating users to migrate to cloud environment.

REFERENCE

[1] Saranya, R., S. Senthamarai Kannan, and N. Prathap: A Survey for Restricting The DDOS Traffic Flooding And Worm Attacks In Intern1et.In:2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT). Pp. 251-256, IEEE (2015).

[2] Worldwide Infrastructure Security Report: Volume XI., https://www.arbornetworks.com/report (2015).

[3] Q1State of the Internet / Security Report, https://content.akamai.com/PG6292- SOTI-Security (2016)

[4] Bhandari, Abhinav, A. L. Sangal, and Krishan Kumar: Destination Address Entropy based Detection and Traceback Approach against Distributed Denial of Service Attacks. In: International Journal of Computer Network and Information Security 7, no. 8 (2015)

[5] Zeb, Khan, Owais Baig, and Muhammad Kamran Asif: Ddos Attacks and Countermeasures Cyberspace. In: Web Applications and Networking (WSWAN), 2015 2nd World Symposium on, pp. 1-6. IEEE, (2015)

[6] N.S. Ali, A. Shibghatullah, "Protection Web Applications using Real-Time Technique to Detect Structured Query Language Injection Attacks", International Journal of Computer Applications (IJCA), Volume 149, paperNo:6, September 2016.

[7] Goadrich M. and Rogers M., "Smartphone Development: iOS versus Android", Proceedings of the 42nd ACM Technical Symposium on Computer Science Education, Dallas, Texas, USA, PP. 607 612, March 2011.

[8] Meier R., "Professional Android 4 application development", third Edition, John Wiley and Sons, Inc., Canada, 2012.

[9] R.Elmasri, S.B. Navathe, "FUNDAMENTALS OF Database Systems", sixth edition, Addison-Wesley, United States of America, 2011.

[10] V. Nithya, R.Regan, J.vijayaraghavan, " A Survey on SQL Injection attacks, their Detection and Prevention Techniques", International Journal Of Engineering And Computer Science (IJECS), Volume 2 Issue 4 Page No. 886-905, April, 2013

[11] A. Alazab, A. Khresiat, "New Strategy for Mitigating of SQL Injection Attack", International Journal of Computer Applications (IJCA), Volume 154, paper No.11, November 2016.