A Secure Methodology to Detect and Prevent Ddos and Sql Injection Attacks

Leelavathy S[a], Jaichandran R[b], Shobana R,[c], Sachin Bhaskaran[d], Aravindh[e] and Prathyunnan[f]

a,b,c,d,e,f
Department of Computer Science and engineering, Aarupadai Veedu Institute of Technology, Vinayaka Missions Research Foundation (Deemed to be University), Paiyanoor, Tamil Nadu, India

Article History: Received: 11 January 2021; Accepted: 27 February 2021; Published online: 5 April 2021

Abstract: As 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) in which filter based approach and software puzzle based approach are performed to detect the malicious script based requests. Once the Deep Packet Inspection (DPI): filter based approach and software puzzle based approach are find satisfactory only the request would be processed. If the request is find malicious automatically the requested IP address would be blocked. Various type 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. This statements are created to make the SQL queries more efficient and render security benefits. This statement provides effective prevention mechanism against SQL injection attacks. 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.

Keywords: Cloud Security, Distributed Denial Of Service, SQL injection, Deep Packet Inspection, Digital Signature Algorithm

1. Introduction

Now a days, all individuals and organisations are migrating their applications to cloud environments so that accessibility made simple but the major concern is the security. Cloud service providers (CSP) providing efficient prevention measures against cloud attacks keeping the data owners file secure may gain confidentiality and trusts among the cloud data owners. In this project, we benefit the stake holders by providing automatic intrusion detection and prevention of two major and common cloud attacks namely DDOS and SQL injections attacks.

This project theme is very important as the attack impact is huge which could take away the organization name to dust and losing all its customer trust and confidentiality. Few recent DDOS attacks are targeted on big brands like GitHub, BBC, Spamhaus, Bank of America/JP Morgan Chase/US Bancorp/Citigroup/PNC Bank, Dyn etc. Also few recent SQL injection attacks are 2016 US presidential election, TalkTalk : a UK-based telecoms company suffered huge data breach, the hardware manufacturer Archos suffered huge loss due to SQL injection attack recently. Thus prevention against these two attacks is more demadful [1] [2].

Distributed Denial of Service (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 internet, online transaction, information exchange is increased significantly. Thus all web based applications has their own database with data owner secret and sensitive information's. 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. They different types of SQL injection attacks are SQL login bypass, blind injection, SQL sleep attack and data fetching attack [3].

Thus in the existing approach all cloud attacks are identified manually and in many cases the network operator doesn't know what are the prevention measures to be performed once the attack happens. Thus to address this problem, automatic intrusion detection and prevention system is needed to detect the malicious scripts with previously trained attack pattern and block the suspicious request and IP of the attacker [4].

2. Literature Survey

[5] Several researchers are contributed towards DDOS and SQL injection based cloud attacks separately. Due to increased number of hackers now a days, a hybrid architecture combining as many cloud attacks into a single application can be of an efficient secure solution. Also many research papers explain these vulnerability attacks theoretically and used simulators for experimental results. Thus real time environment would be much different compared with the simulated results.

[6] As many researches are going on to analyse and prevent DDOS attacks but still there is no successful defence system for DDOS attack has been identified. Many research articles have proposed many methodologies to prevent DDOS attacks. Most common prevention methodology is the signature based technique, in which the machines connected over the network are made up to date security polices based patch update and fix security holes on a regular basis. Another researchers proposed hop count filtering methodology. This is nothing but the network operator maintains complete information of data transmission within the network. They keep a log of information's about the source IP address, its hops from destination are stored in table. If a DDOS intrusion is detected, the network operator can inspect the sender's incoming IP packet's and their respective hops to figure out the spoofed IP packet and the sender details.

[7] Another researcher has proposed, history based IP filtering, in this the network operator keeps a log of a malicious IP in the past from which the attack pattern was detected previously. But the network operator can bale to filter bandwidth based attack traffic only. Thus intruder performing massive DDOS attack cannot be filtered which defeat the server.

Few researchers identified an algorithm to detect high and low rate of DDOS Internet Control Message Protocol Flood (ICMP) flooding. This algorithm would automatically block the IP if it identified I Rate > B Band. Also the algorithm alerts all the IPS when the port alert is triggered. But this algorithm cannot block certain port no which is 0 and also certain ICMP doesn't use port number thus making the proposed algorithm not feasible.

[8] An researcher proposed an prevention algorithm for DDOS flooding attack using certain perimeters. This research used 5 virtual machines assuming both intruder and targeted system are in the same network for the experimental results. The perimeters considered are

1. No. of packets. 2. Packet size. 3. No of machines required for attack. 4. IP address of target machine.

[9] However, the classification phase considers only the outcomes of information gain which will take much time. Also one more researcher proposed k- Nearest Neighbour algorithm to detect DDOS attack. The outcome of the system states whether the packets are normal / malicious. The classification of packets is inefficient due to the consideration of single feature. Thus k-NN classifier classifies based on IP address of the packets but IP addresses are inefficient to detect attacks in cloud system

Few researchers have contributed towards SQL injection attack. In a research paper, they have proposed a proxy parser in between the web and the database servers. This proxy parser inspects the input query and decodes to the correct SQL queries while sending to the database. If the SQL injection is been performed, the proxy parser cannot able to recognise and doesn't pass onto the database raising an alert. The main disadvantage is the proxy parser completely depends on the security of the key and if the key is been compromised, then it makes the proposed algorithm difficult to prevent the SQL injection attack.

In this method, we use netbeans and mysql open source tools for testify our proposed methodology. As these attacks cannot be experimented in real time servers, websites as it would be considered as the cybercrime, we have decided to experiment in the localhost using open source tools. The major phase of our project is to perform the DDOS, SQL injection attacks and integrate the security login to prevent the same attacks within the application using prevention measures. The DDOS attack would be executed in the localhost by generating abnormal burst of requests from the attacker login within the application to attack the netbeans server and SQL injection attack would be executed in the application using SQL queries. In this we analysed four types of SQL injection attacks namely SQL Authentication bypasss, Blind Injection, SQL sleep attack and timing attack. The attack prevention measures adopted for automatic intrusion detection and prevention against DDOS and SQL injection are listed below.

The prevention measures of DDOS attack adopted in our proposed system are Filter Based Approach, Software Puzzle Based Approach and IP validation. In the filter based approach it inspects the incoming packets for any malicious content. In this way vulnerability is reduced. Also to secure the application from bot based DDOS attack and eliminate unauthorised intruder to some level we used software puzzle based approach. If a user requests a service, the respondent server responds to the request once they resolve the software puzzle. This will be generated dynamically. By this process we can eliminate bot based attacks. During the process, if the malicious based packet is detected, the IP address of the attacker would be blocked and prevented from further attack. In this way burst of requests from a single node also would be detected and prevented.[12]

[11] The SQL injection attack is prevented using validating all the fields within the application using prepared statement. If we use prepared statement the intruder cannot able to extract user information from the backend. The prepared statement works on the principle that by using this we can force the user input to be handled as content of a parameter not as the sql command part.

3. Methodology

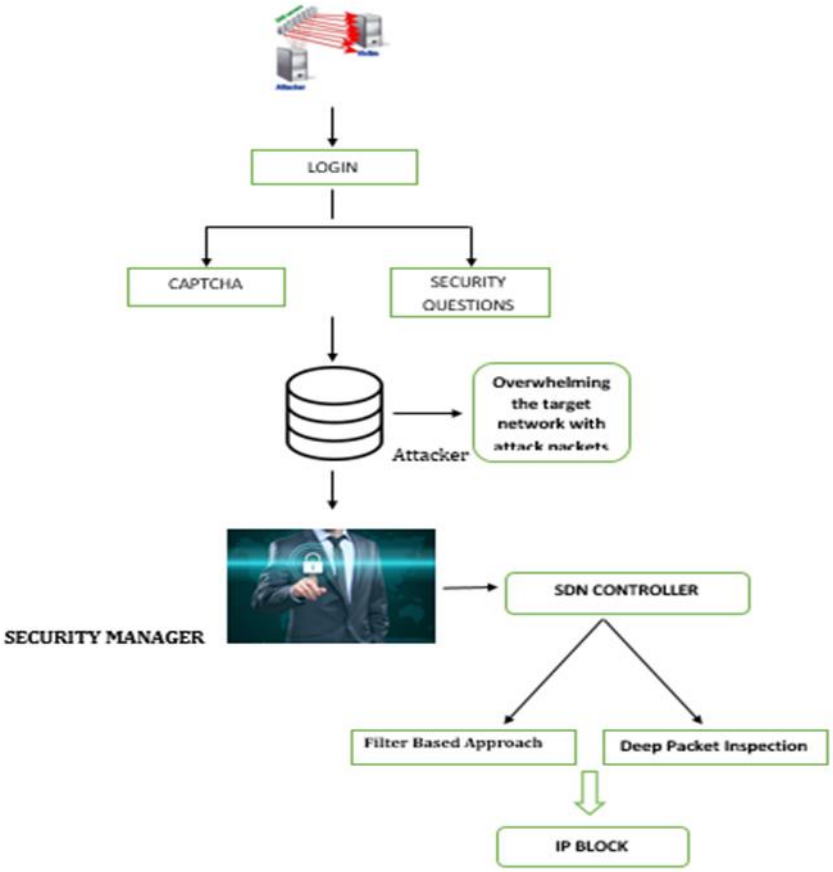

Figure 1 DDOS attack methodology

Figure 1 explains the proposed methodology for DDOS attack patterns within the java server and prevention techniques to detect and prevent DDOS attack using the security login analysing the attack patterns.

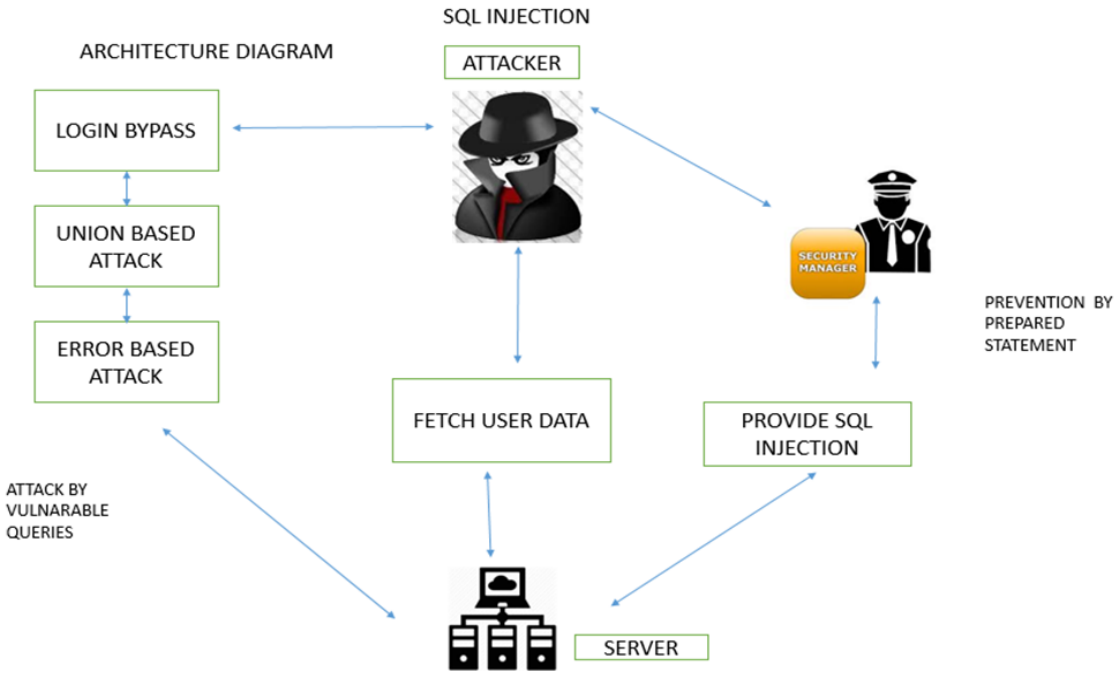

Figure 2 SQL injection attack methodology

Figure 2 explains the proposed architecture to detect SQL injection and prevention measures.

4. Experimental Results

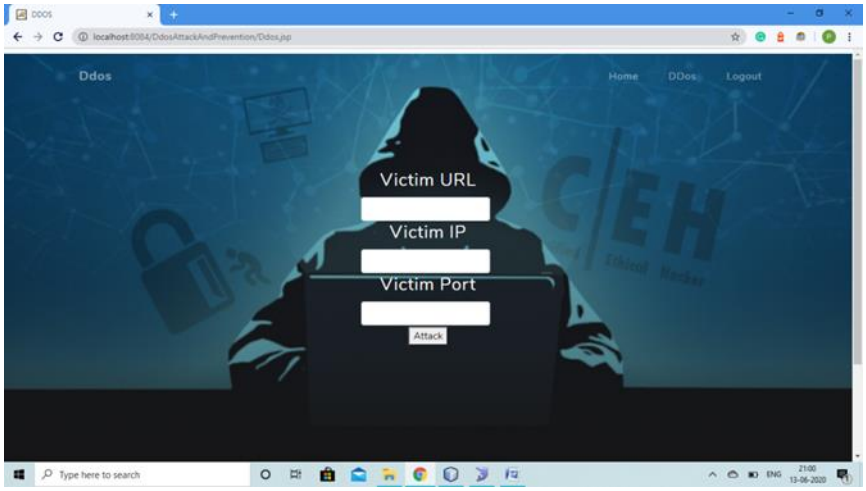

Figure 3. DDOS attack victim device targeting

Figure 3 explains defining the target system IP to burst the request and perform the attack. In the proposed methodology we preforming the attack using malicious scripts.

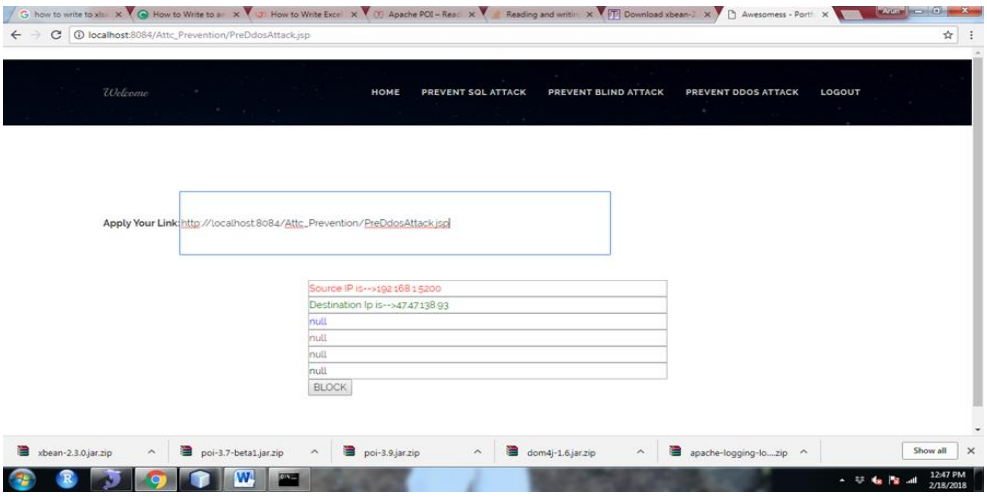

Figure 4. Attacker IP is detected

Figure 4 briefs if the malicious burst of request is detected, the respective IP is blocked to avoid future attack attempts.

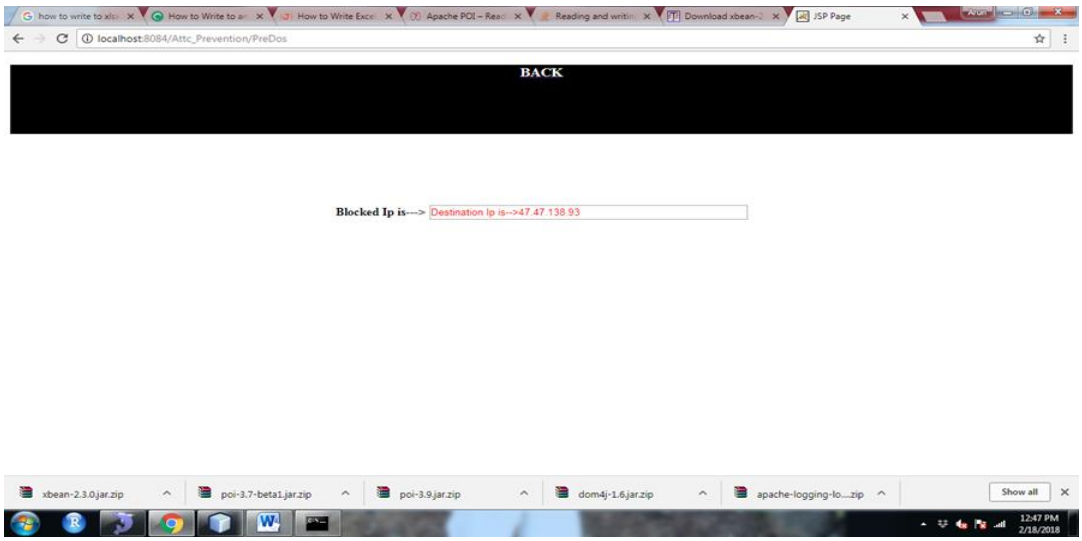

Figure 5. Intruder IP blocked to prevent further attack

Figure 5 explains the list of malicious IP been blocked by our proposed methodology.

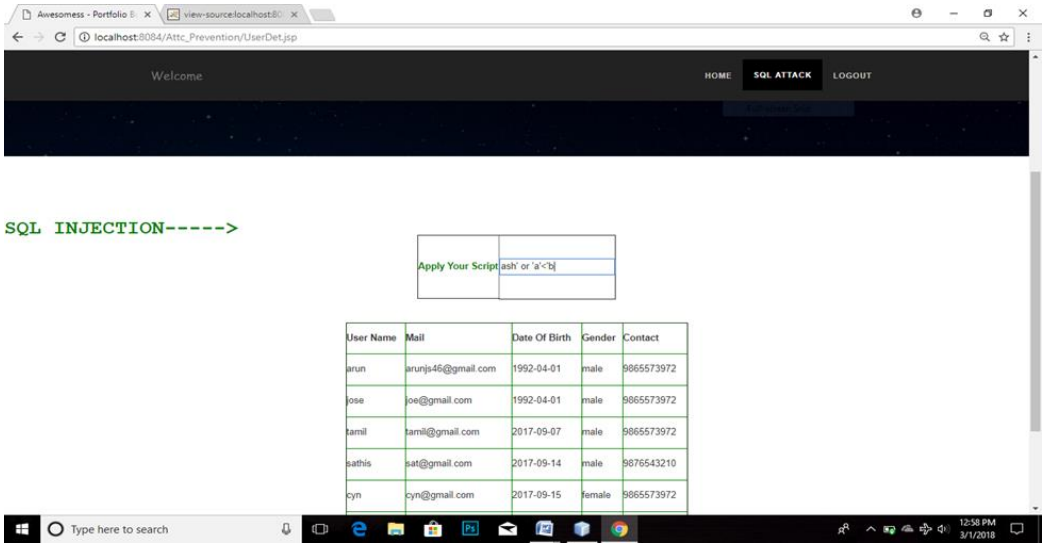

Figure 6. SQL Injection Attack

Figure 6 explains the login bypass SQL injection attack patterns by using the attacker login in our proposed methodology.

5. 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.

References

1. Saranya, R., S. Senthamarai Kannan, and N. Prathap: A Survey For Restricting The DDOS Traffic Flooding And Worm Attacks In Internet.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

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.

11. Raja, K.S., Kiruthika, U. An Energy Efficient Method for Secure and Reliable Data Transmission in Wireless Body Area Networks Using RelAODV. Wireless Pers Commun 83, 2975–2997 (2015). https://doi.org/10.1007/s11277-015-2577-x

12. Rahim, R., Murugan, S., Priya, S., Magesh, S. and Manikandan, R., Taylor Based Grey Wolf Optimization Algorithm (TGWOA) For Energy Aware Secure Routing Protocol.

13. Jayanthiladevi, A., Murugan, S. and Manivel, K., 2018. Text, images, and video analytics for fog computing. In Handbook of Research on Cloud and Fog Computing Infrastructures for Data Science (pp. 390-410). IGI Global.