International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com

An Efficient Technique for Detection and Prevention of SQL Injection Attack in cloud

Shubham Jawanjal[1], Shubham Shegokar[2], Vandana Nandurkar[3], Radhika Ardak[4], Sneha Chaudhari[5], Snehal Rithe[6], Prof. Sneha R. Sontake[7]

[1, 2, 3, 4, 5, 6] *First-Seventh Department of Computer science and Engineering of P.R Pote College of Engineering & Management, Amaravati University.*

Abstract*: Databases are central to the modern websites as they provide necessary data as well as stores critical information such as user credentials, financial and payment information, company statistics etc. These websites have been continuously targeted by highly motivated malicious users to acquire monetary gain. Structured Query Language (SQL) injection and Cross Site Scripting Attack (XSS) is perhaps one of the most common application layer attack technique used by attacker to deface the website, manipulate or delete the content through inputting unwanted command strings. SQL injection attack is one of the most serious security vulnerabilities in Web application system, most of these vulnerabilities are caused by lack of input validation and SQL parameters use. Typical SQL injection attack and prevention technologies are introduced in the paper. We propose the technique to prevent SQL injection attack. Objective of this paper is to re-design the existing available cloud system for running the SQLIA detection and prevention. To detect SQL injection attacks performing its prevention by implementing Apriori algorithm.

Keywords*: SQL Injection, Cloud Computing, Attack detection, Prevention Technique, Apriori Algorithm.*

I. INTRODUCTION

Cloud computing is a new service model which has a great development with the advantages of flexible configuration, on-demand purchase and easy-maintenance. A large number of national infrastructure and related application services are gradually transferred to the cloud computing platform. Although the cloud computing brings many conveniences, it also brings a huge challenge to the security services. SQL injection refers to that the attacker operates the database by inserting a series of SQL statements in the query operation. Gives a feature of SQL injection: "Getting an unauthorized access and immediate retrieval from a database". In recent years, there are many literatures to research the detection and defense of SQL injection attack, but most of them have the low efficiency and high rate of false alarm [1].

To understand the concepts of the cloud computing technology a performance based efficient approach will be required for new paradigms to systematize the usually shared information and to deploy & develop the affiliated changes in different user-oriented platform models. Applying the various but suitable methods for providing privacy checks to the escapes is itself a major challenge of the cloud computing. Web servers which provide customer services are usually connected to highly sensitive information contained backend databases. The incrementing bar of deploying such web applications initiated in ranging the corresponding bar of number of attacks that target such applications. It initiates a vulnerable query to destroy the connected server systems and give attackers unauthorized access to underlying databases & rights to delete, modify and retrieve valuable and confidential information stored in databases.

Problem formalization- Any web application can be formalized with respect to SQL Injection Attack as follows:

A. It accepts the input from user or system.
B. It concatenates input with hardcoded SQL statement and builds complete query structure.
C. Query generated gets executed and concatenates result with HTML code.

In the context of above formalization SQL Injection Attack is targeted on a program at the database layer which is connected to a web application[2].

Vulnerabilities are the weakness which an attacker can take advantage by exploiting it to gain unauthorized access to the target. There are lots of vulnerabilities that can be exploited but three of the most common web application vulnerabilities that exist in a web application are structured query language (SQL) injection, cross-site scripting, and buffer overflow. SQL injection is an attack in which the attacker inserts SQL commands into form or parameter values [3].

II. SQL INJECTION ATTACK

The following example shows how SQL injection attacks realize. SQL injections utilize weakness of a bank's application to misguide the application into running a database backend query or command. Usually, an application of a bank's operation has a menu, which is used for searching customer's personal information, such as the telephone number. The application will execute an SQL query in the database backend.

SELECT client_name, sex, address, date_birth WHERE tel_no=123456 If user enters the string "123456 or 1=1," then the SQL query passes to the database as SELECT client_name, sex, address, date_birth WHERE tel_no=123456 or 1=1. The condition 1 = 1 is always true in database. The query will return all rows in the table, which is not the original intention. The application can be changed so that it accepts one numeric value only. SQL injection attacks can be mitigated by ensuring proper application design, especially in modules that require user input to run database queries or commands [4].

SQL injection attacks pertain to a class of attacks in which user input is molded in such a way so that a part of the query provided by user is SQLIA code. Thus SQLIA tricks the database by passing malicious code to database by embedding it with user input. The attacker injects pieces of malicious software into the databases, which when processed cause data to be executed as a part of command at the backend server, therefore giving undesired results, which are not anticipated by developers leading to compromised security [5].

Objective of this paper is to re-design the existing available cloud system for running the SQLIA detection and prevention. To detect SQL injection attacks performing its prevention by implementing Apriori algorithm. For security purpose we use AES algorithm to modify and update the user Authentication window to detect SQL injection attacks and identify the intruder.

III.SQL INJECTION DETECTION AND PREVENTION

In order to prevent SQL Injection attacks many existing techniques, such as Content filtering, penetration testing, and defensive coding, can be used to detect and prevent a subset of the SQL Injection Vulnerabilities. Over the past years, there has been plenty of research going on in the both academic institutes as well as industries to prevent injection attacks. Following are some prevention mechanism proposed by researchers.

The study [1] proposes a kind of SQL detection method which combined with dynamic taint analysis and input filtering. And it is embedded in the cloud environment to achieve the protection of the Web applications in cloud deployment. First, the method obtains the SQL keywords through the analysis of lexical regulation for SQL statement. Then, it analyses the syntax regulation of SQL statement to create the rule tree. Finally, it traverses ternary tree on the basis of the model which established by SQL syntax regulation to detect the attacks.

The research [2], present a detailed review on various types of Structured Query Language Injection attacks, Cross Site Scripting Attack, vulnerabilities, and prevention techniques. Besides presenting our findings from the survey, it also propose future expectations and possible development of countermeasures against Structured Query Language Injection attacks.

The researchers propose a detection model for detecting and recognizing the web vulnerability which is; SQL Injection based on the defined and identified criteria. In addition, the proposed detection model will be able to generate a report regarding the vulnerability level of the web application. As the consequence, the proposed detection model should be able to decrease the possibility of the SQL Injection attack that can be launch onto the web application[3].

The study[6], proposed a scheme for detection and prevention of SQL Injection Attack using Aho–Corasick pattern matching algorithm. The proposed scheme is evaluated by using sample of well-known attack patterns. Initial stage evaluation shows that the proposed scheme is produce not false positive and false negative. The pattern matching process takes minimum of O (n) time.

The research [7], proposes an efficient technique to prevent SQLIAs and session hijacking attack. The implementation uses hashing technique which is computationally light. The proposed technique effectively prevents SQLIAs and session hijacking attack without much over head on the application.

The study [8] demonstrates a full proof of concept implementation of an ML predictive analytics and deployment of resultant web service that accurately predicts and prevents SQLIA with empirical evaluations presented in Confusion Matrix (CM) and Receiver Operating Curve (ROC).

The research [9], focused on the problem of detecting complex SQL injections. We proposed a novel approach to dissect HTTP requests in order to cover most evasion techniques and improve security rules management process. We also provided an Injection Prevention System architecture which includes a machine learning classifier. A key element of future work is to apply the same approach in order to develop an anti XSS and SQL attacks solution.

IV. METHODOLOGY

This paper proposes an effective method for preventing the SQL injection attack. The method involves the use of Apriori Algorithm. Apriori is an algorithm for frequent item set mining and association rule learning over transactional databases. And for security purposes AES algorithm is used. We propose a technique which work between client side and application server. Every request coming from the client must pass through the protective mechanism before being processed by the application server. If the request contains any of the attacks signatures mentioned in dataset it is illegitimate access to the database. The goal of this work is to prevent illegitimate access to the web application and database.

As you can see from our approach work, the SQL queries are generated by the application server. Our mechanism checks the presence of SQL signatures before the input is processed by the application server.

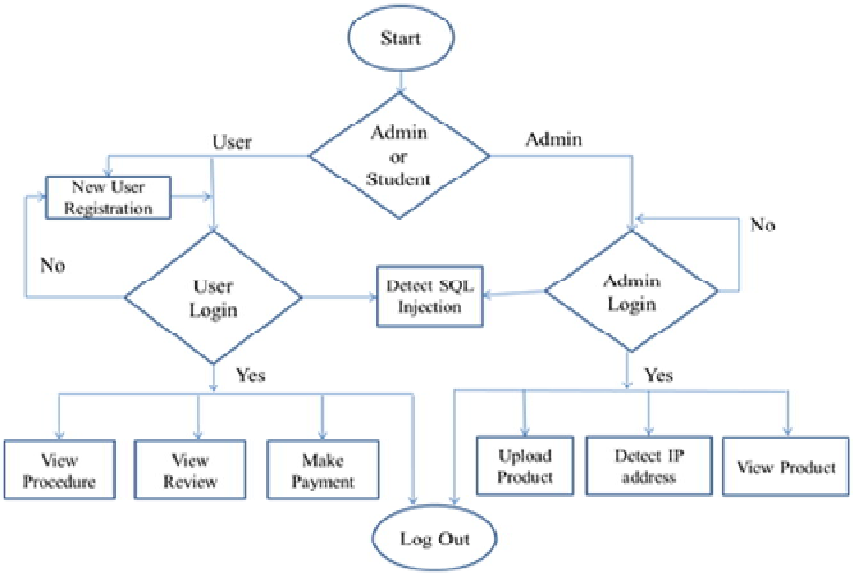

Fig.1 Detection of SQL Injection

Intrusion Prevention can be collaborated with query level access control and data flow analysis to collectively help identify a SQL injection attack with great accuracy. Thus any malicious code present with the SQL query can be easily detected and blocked. Similarly we can integrate intrusion detection with dynamic profiling and event correlation to identify vulnerability of SQL injection attack. In this case any query which does not match the previous data patterns or application model is identified at once. Defensive coding in collaboration with dynamic profiling and intrusion detection may also be used as an accurate method to stop SQL injection attacks.

We maintain a list of known Anomaly Pattern. The user generated SQL Queries are checked by applying Apriori Algorithm. If the pattern is exactly match with one of the stored pattern in the Anomaly Pattern List then the SQL Query is affected with SQL Injection Attack . Then our application don't give access to accessing the Database. For improving the security we using AES algorithm to encrypted and decrypted query.

V. APRIORI ALGORITHM

Apriori is an algorithm for frequent item set mining and association rule learning over transactional databases. It proceeds by identifying the frequent individual items in the database and extending them to larger and larger item sets as long as those item sets appear sufficiently often in the database. The frequent item sets determined by Apriori can be used to determine association rules which highlight general trends in the database.

VI. CONCLUSIONS

The SQL Injection Attack is the largest accessible security risk in Network based computer database in today because all attacker or application programmer attempt to crack the information safety measure accepting similar form of violation. In such a manner

this proposed scheme regarding security against SQLIA, is too sensitive. In this paper we propose the method to detect and prevent the SQL injection by using Apriori algorithm technique and fir security purpose we can use AES algorithm.

REFERENCES

[1] Kuisheng Wang , Yan Hou ,"Detection Method of SQL injection Attack in Cloud Computing Environment ", IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), 2016.
[2] Rahul Johari, Pankaj Sharma,"A Survey on Web Application Vulnerabilities (SQLIA, XSS) Exploitation and Security Engine for SQL Injection ", International Conference on Communication Systems and Network Technologies, 2012.
[3] Geogiana Buja , Kamarularifin Bin Abd Jalil , Fakariah Bt. Hj Mohd Ali ,Teh Faradilla Abdul Rahman,"Detection Model for SQL Injection Attack: An Approach for Preventing a Web Application from the SQL Injection Attack ",IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE), 2014.
[4] Li Qian, Zhenyuan Zhu, Jun Hu, Shuying Liu,"Research of SQL Injection Attack and Prevention Technology ", International Conference on Estimation, Detection and Information Fusion (ICEDIF), 2015.
[5] Pankajdeep Kaur, Kanwal Preet Kour,"SQL Injection: Study and Augmentation",International Conference on Signal Processing, Computing and Control (ISPCC),2015.
[6] M. Amutha Prabakar, M. KarthiKeyan , K. Marimuthu,"An efficient technique for preventing SQL injection attack using pattern matching algorithm", IEEE International Conference ON Emerging Trends in Computing, Communication and Nanotechnology (ICECCN), 2013.
[7] Karis D'silva , J. Vanajakshi , K N Manjunath , Srikanth Prabhu,"An Effective Method for Preventing SQL Injection Attack and Session Hijacking",2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT),2017.
[8] Solomon Ogbomon Uwagbole, William J. Buchanan, Lu Fan,"Applied Machine Learning Predictive Analytics to SQL Injection Attack Detection and Prevention",IFIP/IEEE Symposium on Integrated Network and Service Management (IM),2017.
[9] Abdelhamid Makiou, Youcef Begriche, Ahmed Serhrouchni,"Improving Web Application Firewalls to Detect Advanced SQL Injection Attacks ", 10th International Conference on Information Assurance and Security, 2010.