Detecting Password brute force attack and Protecting the cloud data with AES encryption algorithm

Tejas jadhav[1], Pankaj dhapade[2], Saurabh Mandavkar[3], Shubham shete[4], Dr.Swapnaja Ubale[5]

[1,2,3,4] B.E. Students, Department of IT, Zeal College of Engineering and Research, Maharashtra, India.
[5]Dr.Swapnaja Ubhale , Department of IT, Zeal College of Engineering and Research, Maharashtra, India

---

Abstract

Brute-force attacks are a common occurrence that is becoming more difficult to detect on a network level as the volume and encryption of network data grows, as does the ubiquity of high-speed networks. Despite the fact that research in this sector has progressed significantly, there are still kinds of threats that are undetectable. Because no security solution can ensure that an attacker would not succeed at some point, intrusion detection techniques should be employed to detect abnormal behavior early and reduce the impact of intruders on network performance. This study suggested an intrusion detection technique in which the node (server) monitors network traffic and collects important statistics using a monitoring software application. The administrator will be able to determine whether or not an attack has been carried out by examining and comparing the traffic statistics.

Keywords: - Brute-force, Attacks , Security, Cloud

1. INTRODUCTION

Even with the best technology safeguards in place, such as firewalls and antivirus, information and network systems can be vulnerable to attacks. The reason for this is that information security encompasses not only technological aspects but also other detecting techniques that provide precise analysis. Brute force attacks use random combinations of usernames and passwords to detect login credentials .In recent years, in addition to the well established payload-based detection approach, network security research has begun to focus on flow-based attack detection. Rather than just looking for malicious activities in the actual packet data, network Flows are also examined. This is not surprising, given the lower amount of data to contend with, and the assaults apparent in flow data tend to match the attacks out in network payload. We present a detection strategy and discuss the drawbacks of the flow based attack detection approach . Given research aims to achieve the following points:

1.Encrypting the data by using AES algorithm.

2.Nature of End-Product with the number of login attempts.

3.Information on the initiator of the attack.

The main difficulty appears to be preventing access to unauthorized individuals in order to secure the security of information for the cloud base server with encrypted storage data. Data security should come up with a decent balance between total security and usability. To maintain high security for a user's data when he or she loses access after entering information in the cloud, AES encryption technique would protect the data from hacking or loss.

2. Problem statement

We need to ask ourselves how much secure this kind of services and what would happen to our data if somebody or attacker seized storage servers or hacked into them. Then how much it is really possible to trust in those companies ? .To evaluate the performance of the resultant model, two different test cases were considered; classifying the network connection record as either benign or password Brute-force attack with either all the features or with minimal features.

2.1 Project Overview

In this proposed system , organizations can store data securely on cloud by encrypting it using AES algorithm. We can share data securely on cloud. Here, data was encrypted by sender by using public key and same can be decrypted at receiver side using private key. Therefore though the data was captured by hacker , and he cannot decrypt it until he gets private key, hence data is secure over the cloud.

2.2 LITERATURE SURVEY

Bih-Hwang Lee. [1] explain data security in cloud computing using AES under Heroku cloud. This implementation for deploying Heroku as cloud platform consist of a several steps. This project implements a website as an application to data security. In the website, we implement Advanced encryption standard as data security algorithm. The performance evaluation shows that AES cryptography can be used as data security. Furthermore, delay calculation of data encryption shows that larger size of data increases the data delay time for encrypting data.

Chopade Sonali and Bade Prachi N. [2] explains how organizations can store data securely on cloud by encrypting it using AES and ABE algorithms. We can share data securely on cloud. Here, data was encrypted by sender by using public key and same can be decrypted at receiver side using private key. Therefore though the data was captured by hacker , and he cannot decrypt it until he gets private key, hence data is secure over the cloud.

S. Vigneshwaran and R. Nirmalan. R . [3] explains that the cloud verifies the authenticity of the user without knowing the user's identity before storing data. Attribute based access control has been provided in which only valid users who have matching attributes are able to decrypt the stored information in cloud. The two protocols namely attribute based encryption and attribute based signature were applied to achieve authenticated access control without disclosing the identity of the user to the cloud.

2.3 Research Scope

We proposed an approach for password Brute-force network attacks detection and we can store data securely on cloud by encrypting it using AES algorithm. We can share data securely on cloud. Data is encrypted by sender by using public key and same be decrypted at receiver side using private key. Hence though the data is captured by attacker, and the attacker cannot decrypt it until he gets the private key, hence data is very much secure over the cloud.

2.4 Goals and Objectives

i] Detecting password Brute-force attacks detection.

ii] To encrypt data and store on cloud to protect from hackers.

iii] To provide data security.

iv] To provide access control .

v] To reduce the complexity involved in the key management where the user can be encrypt his/her private data

3. SOFTWARE DESIGN

3.1 Data flow diagram

The data flow diagram (DFD) is a graphical representation of the flow of the data through an information system modelling . A data flow diagram (DFD) is used as a preliminary step to create overview of the system without going into the detail. Context diagram is a top level or LEVEL 0 data flow diagram. It contains a single process node that can generalizes the function of the entire system in the relationship to external entities. data flow diagram (DFD) Layers. Draws a context diagram first, followed by different layers of a data flow diagrams or levels .

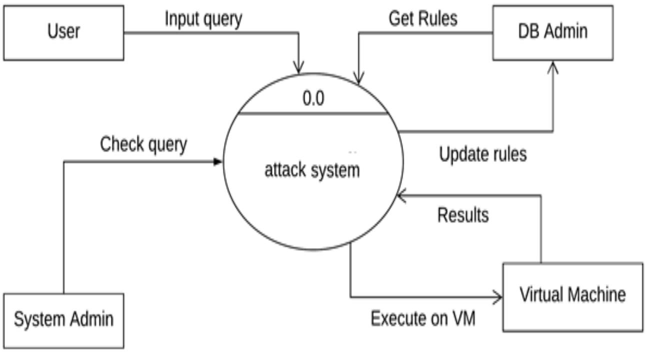


Fig -1: Dataflow Diagram-level 0

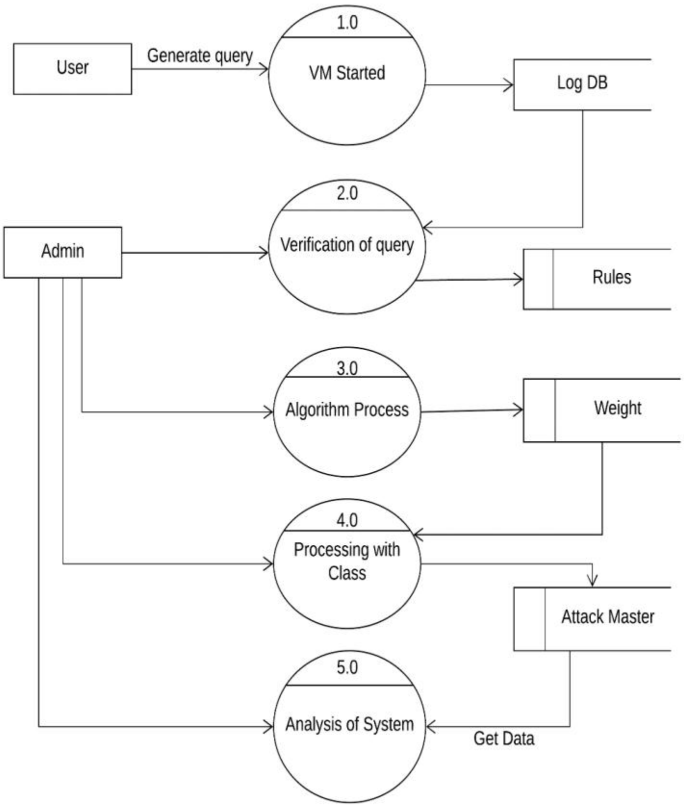
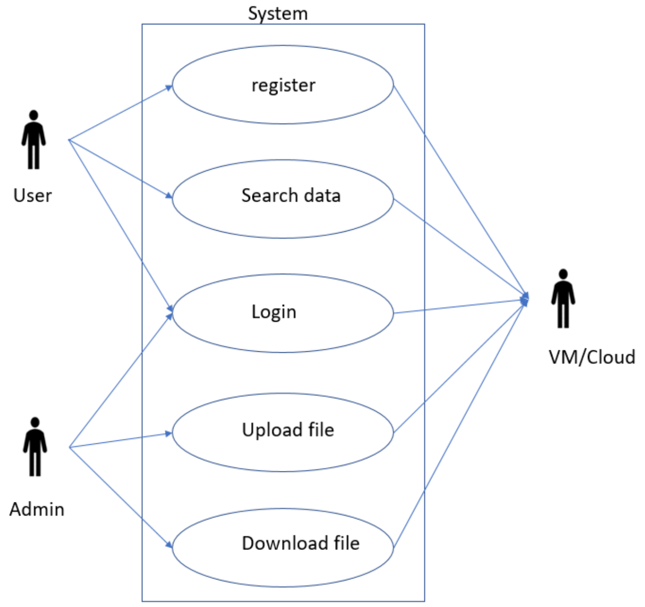


Fig. Dataflow Diagram-level 1

3.2 Use case Diagram

The use case diagrams are used to represent the dynamic behavior of a system. The use case diagrams encapsulates the system's functionality by incorporating use cases, the actors, and their relationship. It also models their tasks, services, and different functions required by a web system/subsystem of a web application. It shows the high-level functionality of the system and also tells reader how the user handles a system.



4. Implementation of AES algorithm

The 4x4 matrix consist of 128 bytes input block is known as the state array. Then the process of encryption revolves around four stages named as mix, columns, sub bytes, add round key and shift rows.

• Sub Bytes

It is defined as substitution step. It is nonlinear. Every byte is restored with another according to the S-box. These operations gives an indirect proportion in cipher. The resultant matrix consists of 4 columns and 4 rows.

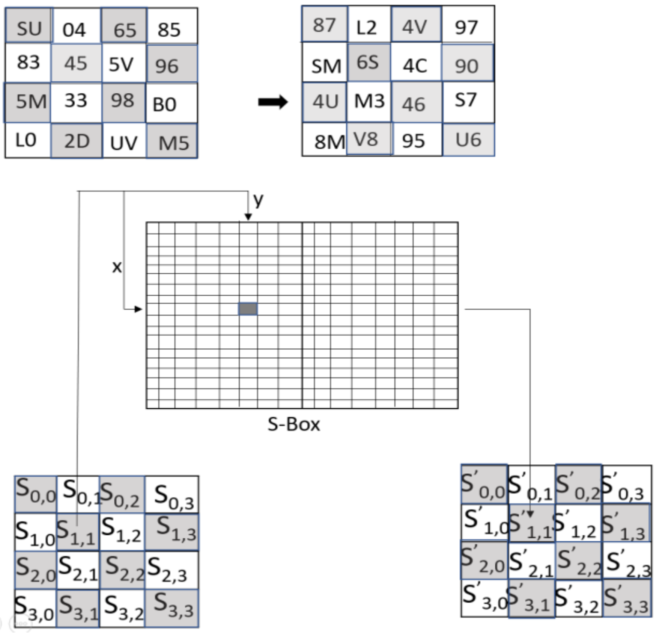


Fig . Byte substitution

• Shift Rows

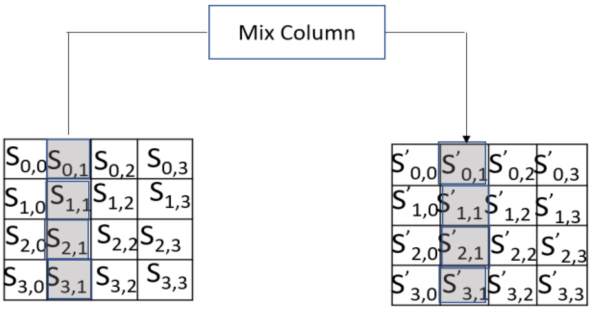
This is the stage where each row is rotated repetitively a definite number of times. It is also known as permutation. The 4 rows in the matrix are rotated accordingly. The rows are shifted to the left. The shift is carried out as Row 1 is not rotated. Row 2 is then shifted one byte place to the left. Row 3 is also shifted two places to the left. Row 4 is then shifted three places to the left. Then the resultant matrix consists of the 16 bytes but rotated with respect to each other.

$$\begin{array}{|c|c|c|c|} \hline B_{0,0} & B_{0,1} & B_{0,2} & B_{0,3} \\ \hline B_{1,0} & B_{1,1} & B_{1,2} & B_{1,3} \\ \hline B_{2,0} & B_{2,1} & B_{2,2} & B_{2,3} \\ \hline B_{3,0} & B_{3,1} & B_{3,2} & B_{3,3} \\ \hline \end{array} \rightarrow \begin{array}{|c|c|c|c|} \hline B_{0,0} & B_{0,1} & B_{0,2} & B_{0,3} \\ \hline B_{1,1} & B_{1,2} & B_{1,3} & B_{1,0} \\ \hline B_{2,2} & B_{2,3} & B_{2,0} & B_{2,1} \\ \hline B_{3,3} & B_{3,0} & B_{3,1} & B_{3,2} \\ \hline \end{array}$$

Shift Row

• Mix Columns

In mix colunms step , every column is changed using matrix multiplication. Each column consists of four bytes. The resultant matrix consists of 16 bytes. The input is taken for each column. It takes four bytes. Then the output produces four bytes which is entirely different from the four bytes given as the input



$$\begin{pmatrix} S'_{0,1} \\ S'_{1,1} \\ S'_{2,1} \\ S'_{3,1} \end{pmatrix} = \begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} S_{0,1} \\ S_{1,1} \\ S_{2,1} \\ S_{3,1} \end{pmatrix}$$

Fig .Mix Columns

• Add Round Key

Round key is bounded to each and every byte of state. In step, the matrix is XO-Red with the round key. A 4x4 matrix represents the original key. It contains 128bits. This four words key where each word is of 4 bytes, is converted to a 43 words-key. The first 4 words represent W[0], W[1], W[2], and W[3].

4.1 System Implementations

The proposed system is designed to maintain security of not only (.txt) files but also (.pdf) files . Given proposed system uses Advances Encryption Standard algorithm to perform encryption and decryption . When Admin uploads the pdf or text files in Cloud Storage, the file is encrypted . Inverse of the AES algorithms are used to decrypt the file when the user downloads it from Cloud Storage .

4.1.1 Password brute-force attack detection

Website applications are widely used in many enterprises, while they are providing convenience, the web application brings a lot of the security risks. Password is the first line of defense in the web application, the low level password problem has always been a short board in web application security protection system.

In this system user should create an account , admin account credentials are default . when the attacker tries to brute-force the password using any method . The admin and user both will be notified after certain number of wrong passwords attempts . After detecting the attack admin will have the rights to block the IP address of the attacker .

4.1.2 Admin Panel

In this system, Admin has the authority to edit, modify, create, share and restrict access to the cloud data. Admin is the one who wants to spread his business with the help of website then he/she has to set up the servers and maintenance of servers which leads to the high cost. In this system, the Admin can access and archive the data stored by the Cloud Service Provider .

• User sends a key request to Admin and intern to the cloud.

• File upload section is where the user uploads files either of (.txt, .pdf) format. The file is then encrypted using the key generated by AES algorithm in the cloud/virtual machine.

• Encryption section of this module encrypts text files .This module uses AES algorithm to generate encryption.

• When Admin uploads the text files in Cloud Storage, the file is encrypted. Inversing AES algorithm the file can be decrypt when the user downloads it from Cloud Storage. This increases the security.

4.1.3 User Panel

Data user uses the cloud to access data stored by Admin at any point of time. Admin will share the data requested by user stored on the cloud database .

• The users can search for their required files present in the cloud storage. These files are uploaded by the Admin. They are present in encrypted format. Hence,user must request Admin for key to decrypt the file and download it.

• The request for key can be sent in the key request page of this User panel.

• Using the key sent by Admin, the user can decrypt the file and download it.

5. Conclusion

In this study, we proposed an approach for Password Brute force attacks detection based on a AES encryption algorithm. The raw data was converted into files and then used for model training and testing.

The data is also been made secure as uploaded file are been converted in encryption form and stored and for decryption of those file user requires the key to view the file in original format .The experimental results showed that our model detects benign and Password Brute force attack with higher accuracy and precision when all the features in are used.

6. REFERENCES

[1] Bih-Hwang Lee “Data Security in Cloud Computing Using AES Under HEROKU Cloud” 2018 IEEE.

[2] Chopade Sonali and Bade Prachi N “Secure Cloud Data Using Attribute Based Encryption”2019 IEEE.

[3] S. Vigneshwaran and R. Nirmalan. R “Attribute based Encryption on Secret Verification in Cloud ” 2015.

[4] Yujiao Song , and Hao Wang “Efficient Attribute-Based Encryption with Privacy-Preserving Key Generation and Its Application in Industrial Cloud ” 2019.

[5] Avinash N and Divya C “An Attribute Based Encryption for Accessing Data on Cloud ” IEEE .