Amalgamation- Data Redemption Model

[1]Priyavarshini C U, [2]R.Harish kumar, [3] Mrs.S.krishnaveni
Student, Student, Assistant Professor
Software Engineering
SRM University, Chennai,

Abstract-Data security means protecting data, such as a database, from destructive forces, and from the unwanted actions of unauthorized users. The growing popularity of the Internet in homes means that computing has become network-centric and data is now available outside of disk-based digital device. Security in terms of integrity is most important aspects in cloud computing environment. In this paper, a detailed analysis of the data security problem is presented. We tried to solve problems if the attack has been made already on the data and also to provide information from where the attack has been made, we present a secured solution to solve the problems which can ensure the efficiency and security of the system. To ensure the security of data we proposed a method by implementing Token based Authentication

Index Terms- Cloud computing, Token based data security.

I. Introduction

The purpose of the project is to secure data from the hackers and collect information of the hacker. Internet usage has increased exponentially and has managed to cover all geographical areas across the globe. So the match between security experts and hackers is still on, as each overcomes the other again and again. We proposed a model to overcome this problem. When the user uploads the data in cloud server, the security is provided using token key authentication. When someone tries to access your data, it will erase the data and sends the information about the hacker and erased data to the user which will help us from further attacks.

There are two types of users in the system- normal user and business user. Both of them have certain functions specific to them. The common functionalities are that the users being able to set up their profile with their profiles information. The business user will have more security as the database of the application has to be secured more.

The main perspective of the project is to secure the data saved in the cloud platform. Nowadays, internet hack attacks have become increasingly rampant, and hacker's technical means are also increasingly complicated. Many government departments, research institutions, military departments and key enterprises etc. have become the main target of hacker attack, hackers' illegal conduct have caused irreparable disaster and wastage to society and business.

To overcome these issues we proposed a system which will ensure the security of the data and also provides evidence of the hacker who attempts to attack the system and capture the data. When the hacker tries to access the data, the data gets deleted by the program by creating content file at the back of the file to be accessed. Then it mails the ip address of the hacker and trigger message of the file that was tried to be accessed to the user.

II. Related works

In the existing system it contains two engines, network evidence capturing engine and network forensics analysis engine. The network evidence capturing engines are used to capture the intrusion and invasion process and log them, then the log is quickly sent to the network analysis engine for the detailed analysis of the file type and then the protocols are used to protect the same type of files from further attacks of the intruder. Application data recovery analysis is to analyze the application data from the network data files, such as the WWW records, email records Telnet records and FTP records.

This solution can not only find out intrusion behavior from log information of network data using both static analysis and dynamic analysis methods, but also can transfer system log to the forensics device to prevent hackers to delete the log. This system can record all the network data that across the being forensic computer and store them with time period in accordance with the requirements of the law evidence, so that intrusion behavior will be found out by packet analysis. This processing mode can ensure data integrity and original, so the analysis results of the data possess a high degree of credibility.

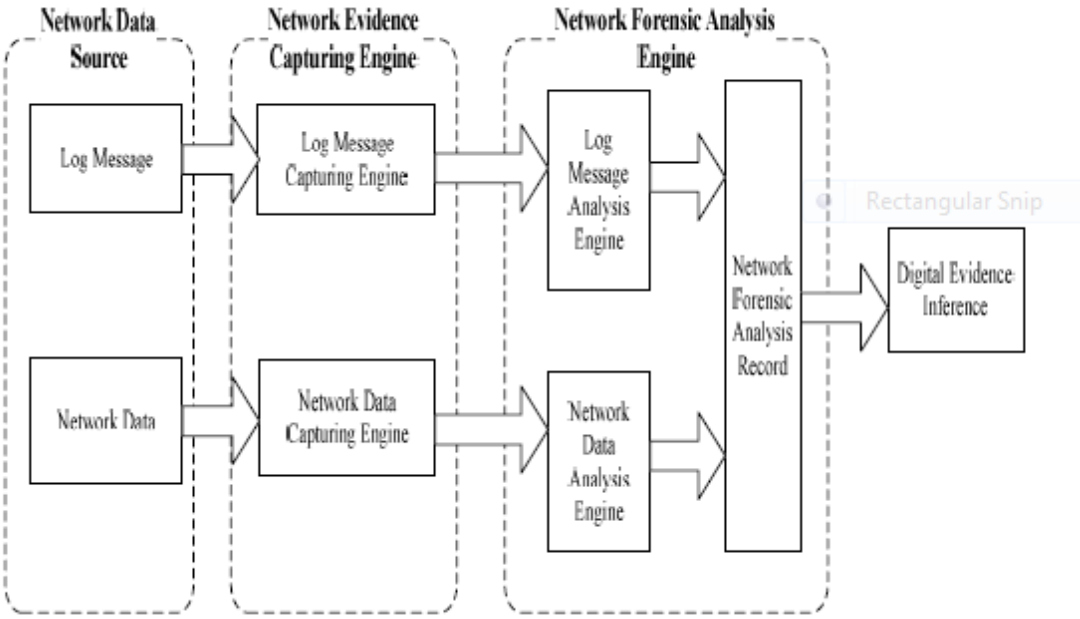


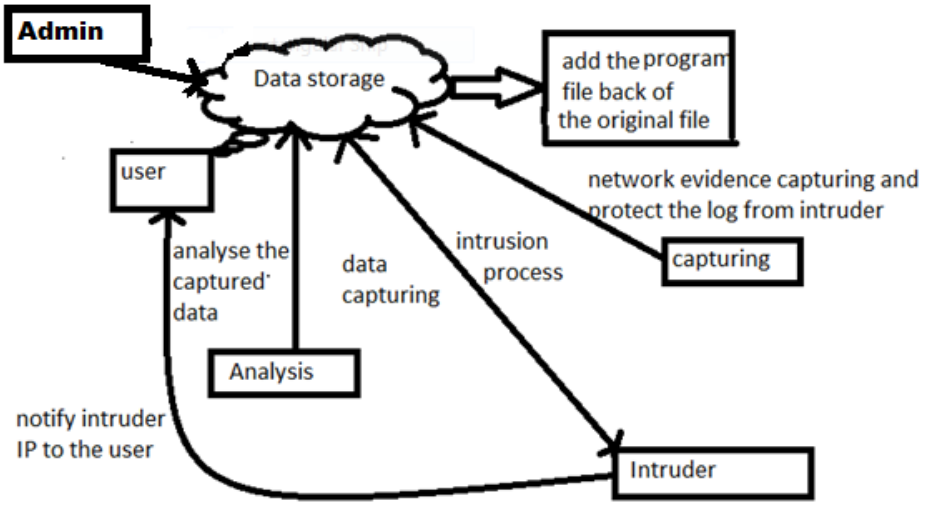
Figure 1: existing system architecture diagram

In case if the hacker somehow accesses the file system; there are no ways to protect the privacy of the data. The system fails to protect the data from the first attack. And also no trace of intruder is sent to the authority. The paper mainly focused on the preventive issues; it did not state any ways or protocols to protect the security and confidentiality of the data files.

III. Proposed System

In this paper, we proposed a technique which protects the content of a file from the intruder.

The algorithm called blowfish will add a program file at the back of the original file and it is hidden**.** The program file contains Clear-Content command. The Clear-Content cmdlet enables you to erase the contents of a file without deleting the file itself which is enabled when it fails to satisfy authentication and security protocol.



When the content of a file is erased, it will send the notification to the user with the details of the file and from which IP address it is downloaded will be mentioned in that notification.

The file which is deleted is redirected to the other channel in the same server. There is a slight variation in the type of user which we chose for uploading the file. The business user will be aware of the attack on the file from the admin. But normal user will come to know only if he/she notices that the file is missing.

The data is encrypted and decrypted using blowfish algorithm which is a symmetric key algorithm. It uses same key for encryption and decryption. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date.

There are three main features in the system.

Authentication:

The user is provided with the proper authentication using user name and password. Hackers will not possibly open the attack unless the user is careless.

Secured data

Once the data has been saved in cloud environment, the data will be protected. If the hacker tries to access the data, the data will immediately be deleted by creating content file using clear content cmdlet. And it will be redirected to the other channel which will be notified to the users.

Notifications

When the hacker attacks the data , the ip address of the hacker and information of the file which is has been downloaded will be sent as a mail to the user as a trigger message. Admin will come to know where the data has been redirected.

IV. Module Description:

Module 1: Registration

The users will be classified into one of two types- user, business. Both of them have certain functions specific to them. The common functionalities are that the users being able to set up their profile with their profiles information. The business user will have more security as the database of the application has to be secured more

Module 2: Login

The username and password will be asked after registration after registering their account. After entering right credentials, the page will be preceded to the user's profile which contains the upload system where user can upload the file with the token key which is unique to individual user.

Module 3: Upload file

To upload the file , we need to enter the user name and cloud id is generated for each user .To upload the file , click on the upload button which will lead us to the file browser To cancel uploading, we give clear button on the page.

Module 4: Uploaded file

In this module, the files which are uploaded by the business or normal user will be displayed. The users can either delete the file or download the file. To download or delete the file, the token key is asked which our next module.

Module 5: Token key

The token key is used to prove one's identity electrically. The token is used in place of the password to prove that the customer is who they claim to be. To download or delete the file, you need this token key 9in our project. This token key is generated during registration.

V. Conclusion

In this paper, we have presented solution which will protect the contents of the file from the hacker after the attack and also obtains the IP address of the intruder which will help the authority to know from where the file has been hacked and it also prevents from the further attacks from the intruders.

References

[1]. Applying Agents to the Data Security in Cloud Computing Feng-qing Zhang, Dian-Yuan Han Computer Engineering School, Weifang University, Weifang 261061, Chinae-mail:zhangfq@126.com

[2]. Da-Wei Sun, Gui-Ran Chang, Shang Gao. Modeling a Dynamic Data Replication Strategy to Increase System Availability in Cloud Computing Environments. Journal of Computer Science and Technology 27(2): 25 6-272 Mar. 2012

[3]. Design and Implementation of Network Forensic System Based on Intrusion Detection analysis.

[4]. 2012 International Conference on Radar, Communication and Computing (ICRCC), SKP Engineering College, Tiruvannamalai, TN., India. 21 - 22 December, 2012. pp.171-175.

[5]. YAO Li-hua,SHAO Jian, SHENG Guo-qiang,ZHANG Guo-xuan *Hangzhou Dianzi University,Hangzhou,China,310018 Lihua728824@163.com on* Research on a Security Model of Data in Computer Supported Collaborative Design Integrated with PDM System.

[6]. Amitava Nag, Saswati Ghosh, Sushanta Biswas,Debasree Sarkar, Partha Pratim Sarkar 2012, "An Image Steganography Technique using X-BoxMapping", *IEEE Xplore Digital Library, International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012.*

[7]. O ¨ . Durmaz Incel and B. Krishnamachari, "Enhancing the Data Collection Rate of Tree-Based Aggregation in Wireless Sensor Networks," Proc. Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON '08), pp. 569-577, 2008.