ISSN: 2278-4632
Vol-10 Issue-6 No. 8 June 2020

AN EFFICIENT APPROACH FOR DATA ATTACK IN THE CLOUD USING MITIGATION METHOD

Akhila H Kumar[1] and Komarasamy G[2]
PG student[1], Associate professor[2]
Department of Computer Science and Engineering
Jain (Deemed –To –Be University), Bangalore, Karnataka
akhilahkumar27.8.1997@gmail.com, gkomarasamy@gmail.com

Abstract-Cloud security, also known as cloud computing security, consists of a set of policies, controls, procedures and technologies that work together to protect cloud-based systems, data, and infrastructure. These security measures are configured to protect cloud data, support regulatory compliance and protect customers' privacy as well as setting authentication rules for individual users and devices.It is going to propose a different approach for securing data in the cloud using AES Encryption scheme.The way cloud security is delivered will depend on the individual cloud provider or the cloud security solutions in place. Cloud data security becomes increasingly important as to move the devices, data centers, business processes, and more to the cloud. Ensuring quality cloud data security is achieved through comprehensive security policies, an organizational culture of security, and cloud security solutions.

Keywords: cloud data security, data theft, AES encryption ,personal data.

1. INTRODUCTION

Presently days in a business world cloud is utilized to store the more secret information. Here data security is exigent issue in the cloud. Data Theft Attacks have frequently happened in the cloud, so most business zones know about security issues. Most of the capitalized evolution failed to look after the security in the cloud especially in business zones. So here it is going to focus on this issue based on data theft attack in the cloud by figuring out the security issue.

As most of the customer are well aware of this threat in the cloud,here it is left only with trusting the service provider when it comes to protecting their data. So for this lack of transparency, it can control over alone by having the knowledge of cloud authentication[1], along with the data transmission [2],authorization and along with the audit controls which can get the solution for this problem. In the earlier days, it was very easy to stole someone's admin password which can be outsider or insider, so for this problem here it is going to show how Cloud customers' private keys might be stolen and how some confidential documents/files can be extracted from hard disk. After stealing the password by the malicious person(outsider/insider),malicious person gets the access of the customer's data, while that time customer doesn't require to bother about detecting the unauthorized access.

2. LITERATURE REVIEW

2.1 Authentication

In order to make data scalable and secure in cloud environment researchers proposed several methods. This paper[3]suggests the authentication and data theft attacks which have been solved by the concept of cryptography analysis and AES. Here it have used the concept of cryptography analysis for the authentication purposes and for data security purposes they have used the concept of AES encryption scheme.

2.2 Security

As this paper [4] suggest the security of the data based on health care application with content sensitive access in IOT by using the concept of secure mutual authentication approach. To improve security issues like data privacy, data transmission being used and it is totally depends upon the users which needs to be careful before any interaction.

2.3 Data Transmission

The authors from the paper [5]got the idea of applying the concept of fog computing and the IOT for securing the data security and data transmission and the as the authors got motivated from the research from the concept of Service Oriented Architectures (SOA) the iTaaS solution makes use of modular services implementing fundamental functionalities communicating with each other .

So here the data will be encrypted under a set of attributes and multiple users decrypt their data using assigned key "B. M. Bowen and S. Hershkop, "Decoy Document Distributor: http://sneakers.cs.columbia.edu/ids/fog/," 2019. [Online]. Available: http://sneakers.cs.columbia.edu/ids/FOG/".

ISSN: 2278-4632
Vol-10 Issue-6 No. 8 June 2020

2.4 Monitoring and Management of data

This section describes about some research works focused on monitoring and management in cloud and cloud computing denotes an architectural shift toward thin clients and conveniently centralized provision of computing resources. Clients' lack of resource control in the cloud occasion concern about the potential for data privacy issues, particularly abuse or leakage of sensitive information by service providers. Cryptography is a proclaim remedy. Among its one of the most powerful primitives is fully homomorphic encryption (FHE)scheme[6,7], dubbed by some the field's "Holy Grail," and recently realized as a fully functional construct with seeming promise for data privacy. As recently got realization based on the concept of cryptography analysis, alone can't enforce the privacy demanded by common cloud computing services, even with such powerful tools as FHE encryption scheme.

2.5 AES Encryption Scheme

By defining a hierarchy of natural classes of private cloud applications, and show that no cryptography protocol can implement those classes where data is shared among clients. It will also need to rely on other forms of privacy enforcement and security in data[8], such as tamper proof hardware, distributed computing, and complex trust ecosystems. As like any anomaly-detection based techniques, detecting masquerade attacks by profiling user behavior suffers from a significant number of false positives. This is going to extend the prior work and provide an integrated detection approach in this paper. Masquerade attacks are identified by an antagonist stealing a legalized user's credentials and using them to imitate the victim and perform malicious activities, such as stealing information. So here this is going to combine a user behavior profiling technique with a provoking technique in order to more accurately detect masquerade attack.

It will show that using this integrated approach reduces the false positives by 36% when compared to user behavior profiling alone, while attaining almost perfect detection results. Furthermore, it is going to show how this combined detection approach can serve as a mechanism for solidifying the masquerade attack detector against mimicry attacks.

3. EXISTING SYSTEM

Existing data protection mechanisms such as encryption have failed in preventing data theft attacks, especially those perpetrated by an insider to the cloud provider. Cloud computing security[9] do not focused on ways of preventing the data from unauthorized access. The authors also demonstrated how cloud customers' private keys might be stolen, and how their confidential data might be extracted from a hard disk. After stealing a customer's password and private key, the malicious insider get access to all customer data, while the customer has no means of detecting this unauthorized access. Here in the existing system cloud computing security solution which is cryptography analysis which was having the belief of securing the data which is stored in the cloud and tried ti get the best user behavior profiling in the web technology and along with the prevention of stored data in the cloud which is stored.And here in the cloud data security ,the block chain approach[10]and for security purposes ,resources allocation[11] also have been used but the data integrity becomes failed but they got success in data availability and data confidentiality.

Here the existing system talks about the cloud privacy which had tried to proof the cloud privacy can be done by using the concept of cryptography analysis methodology but it got failed to proof so by taking this issues ,here got an idea to proceed on the concept of decoy information technology due to attacks occurred in the cloud in the recent years and this becomes good at the time when the users started to use it but it got failed due to some of the dangerous attack and by using the algorithm called DSV ,in the recent years data theft attack in the cloud but by using this algorithm it showed about the prevention done against the APT(Advanced Persistent Threats)but still some of the social media websites gets attacked by these threats.The disadvantage of this approach is providing security of confidential information remains a core security problem that, to date has not provided the levels of assurance most people desire.

4. PROPOSED SYSTEM

The proposed system completely different approach to securing the cloud using AES encryption scheme. We use this technology to launch misinformation attacks against malicious insiders, preventing them from distinguishing the real sensitive customer data from fake worthless data.The advantage of using this method is detection of masquerade activity, confusion of the attacker and the additional costs incurred to distinguish real from bogus information and the deterrence effect which, although hard to measure, plays a significant role in preventing masquerade activity by risk-averse attackers.In this approach, we are using the web technology which is based on the servlet, JSP(1.7)based, web server here we are using the Tomcat(6.0) based server and here database is being used from My SQL(5.0) along with the IDE which is Eclipse Galileo based and for the connection we have used the JDBC Type4 and for UGI for database, we used the SQLYog with coding language which is JAVA (jdk1.7).

4.1 Non- Functional Requirements

i. Feasibility Study

Feasibility is the determination of whether or not a project is worth doing. The process followed in making this determination is called feasibility Study. This type of study if a project can and should be taken. In the conduct of the feasibility study, the analyst will usually consider seven distinct, but inter-related types of feasibility.

ISSN: 2278-4632
Vol-10 Issue-6 No. 8 June 2020

ii. Technical Feasibility

This is considered with specifying equipment and software that will successful satisfy the user requirement the technical needs of the system may vary considerably but might include:

- The facility to produce outputs in a given time.
- Response time under certain conditions.

iii. Economic Feasibility

Economic analysis is the most frequently used technique for evaluating the effectiveness of a proposed system. More commonly known as cost / benefit analysis. The procedure is to determine the benefits and savings are expected form a proposed system and a compare them with costs. It benefits outweigh costs; a decision is taken to design and implement the system will have to be made if it is to have a chance of being approved. There is an ongoing effort that improves in accuracy at each phase of the system life cycle.

iv. Functional Requirements

To propose a completely different approach to securing the cloud using AES encryption scheme.By using this technology to launch misinformation attacks against malicious insiders, preventing them from distinguishing the real sensitive customer data from fake worthless data. In the figure 1 illustrates J2EE technology and MVC design pattern can simplify the software development, improve the software performance and quickly construct the dynamic E-business system of the good expand, maintainability, dependability and high usability. The traditional system of industry report is highly influenced by the database security and has low efficiency .

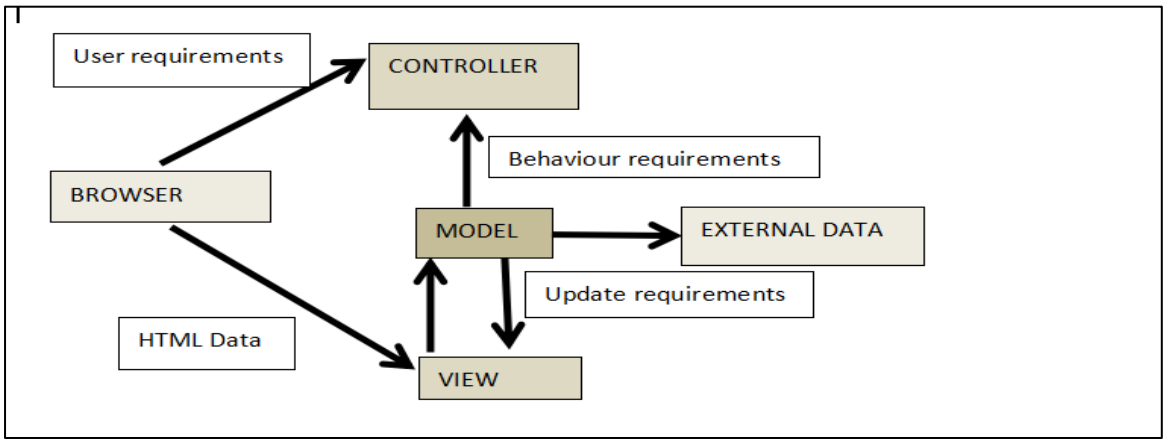


Fig 4.1 J2EE uses MVC Architecture

Fig 4.1 illustrates J2EE technology and MVC design pattern can simplify the software development, improve the software performance and quickly construct the dynamic E-business system of the good expand, maintainability, dependability and high usability. The traditional system of industry report is highly influenced by the database security and has low efficiency

v. Creation of user profiling:

In this case, once the admin logged in ,the user need to follow some ways as user need to create their own user creation in which admin have privileges to create the user ,while that time he/she need to send the user id and user password in user's email-Id. And the second task is based on the user's details in which they have permission to edit , delete and view any numbers of user's.

vi. Maintenance of Cloud Configuration (View):

In this approach after the process of profiling of user details and information and sending the user id and user password to the user's email id, now he/she need to maintain the cloud configuration of server by having the detailed format as date and time.

vii. Upload the File (with subject):

Admin uploading the file into cloud storage that files should be encrypted by using AES algorithm. Once admin uploads the file it gets stored in original file storage at the same time a dummy file is being created with the same name as original file but bogus contents and uploaded to duplicate file storage. N this approach he/she can view the uploaded all files and along with the detailed information with date and time to the cloud server.

viii. Master Key Generation and Change Password:

As in this concept the admin can generate Master AES key which is an encryption scheme that is used to encrypt the file which he/she wants to upload to cloud. He/she can change his/her password by entering Current and new passwords.

ISSN: 2278-4632
Vol-10 Issue-6 No. 8 June 2020

In this situation, if once the user logged in he/she has to follow two instructions that first is login and second is for downloading the file, here firstly user has to get the user id and password through email. User can able to login by using user id and password and secondly, checks for behavior here for the particular user who is requesting for file download, application will check how many files he downloaded on that day let it be N. Get no of files allowed to download for the user from user table let it be M. If N<= M then Correct Behaviour else Misbehavior. Suppose the user wants to download any file, first he has to select the file from the list and, then decrypt the using AES key and store into the local system. In Change password, User can change his password by entering old and new passwords.

5. EXPERIMENTAL RESULT

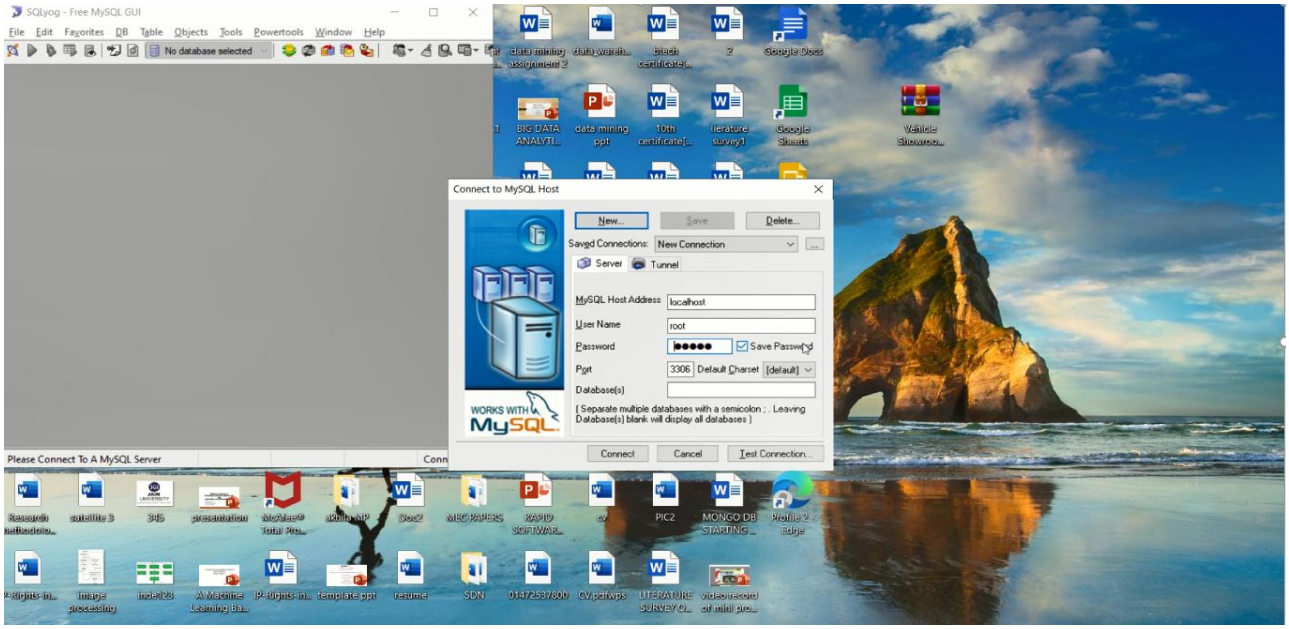


Fig 5.1 Connection between the MYSQL and SQLYog

Fig 5.1 illustrates the connection between the MYSQL and SQLYog in which they asks for the username and password for get connected to the SQLyog for getting the information about the user details whether they are insider/outsider malicious to know and along with the uploaded files details and to identify the files are correct or wrong and it also tells about the the behaviour who had logged in the web application ,here they identifies the behaviour of user.

Fig 5.2 illustrates the files which are uploaded in the web application they gets stored in the cloud service provider along with the date and time and the size of the file which they are already connected with the Tomcat web application manager.

Fig 5.3 illustrates detailed information of each user with time and date and also about the uploaded files in the SQL with the detailed information like behaviour of the user whether they did misbehave or behave properly,date of the uploaded files by the user ,time of the uploaded files by the users, along with the uploaded files with null notes inside them, etc.

ISSN: 2278-4632
Vol-10 Issue-6 No. 8 June 2020

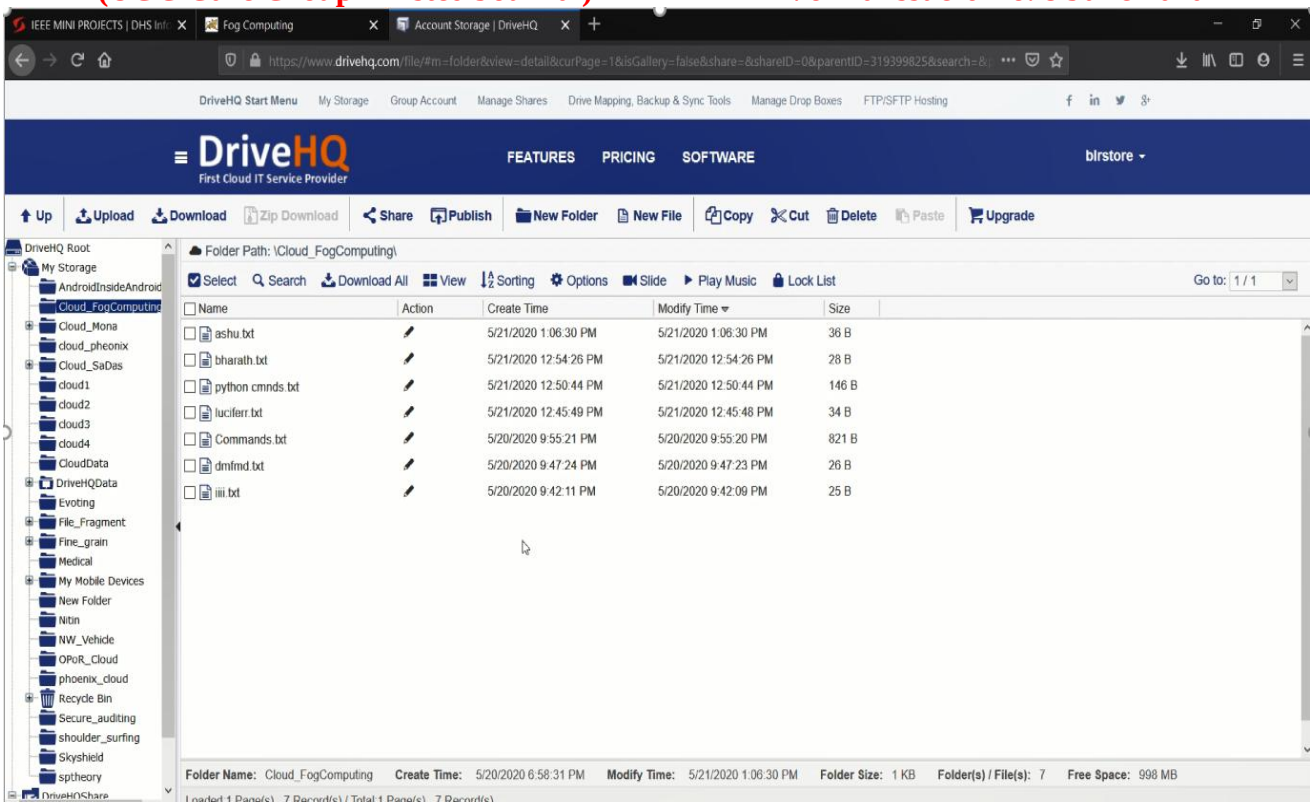


Fig 5.2 Uploaded files in the cloud

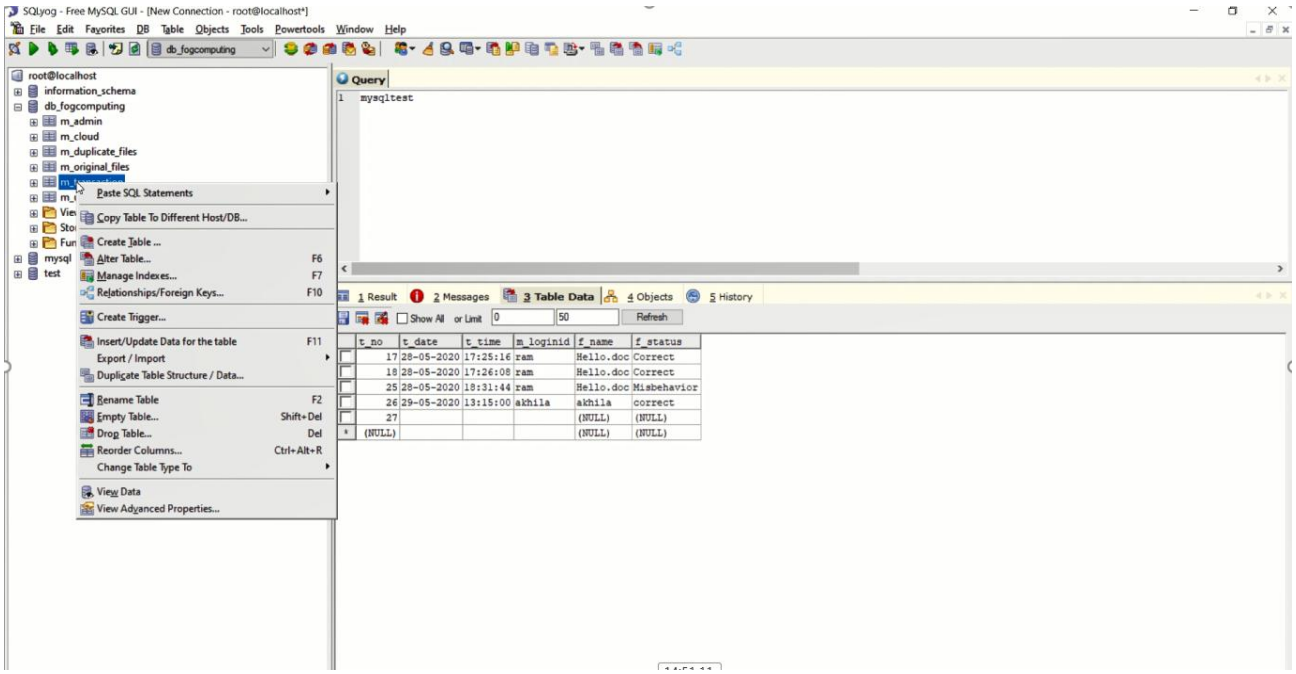


Fig 5.3 Detailed information with time and date

Fig 5.4 illustrates connection of tomcat application manager in this figure they tells the connection is done when the MYSQL and SQLyog gets connected to each other to create the user profile and get the entry in the web application called Tomcat application manager.

Fig 5.5illustrates about the master key generation and changing the password and along with that they tells about the user can change the password after uploading your files/documents in which, when the user clicks on the AES key which is used for encrypting the files which are already uploaded.

ISSN: 2278-4632
Vol-10 Issue-6 No. 8 June 2020

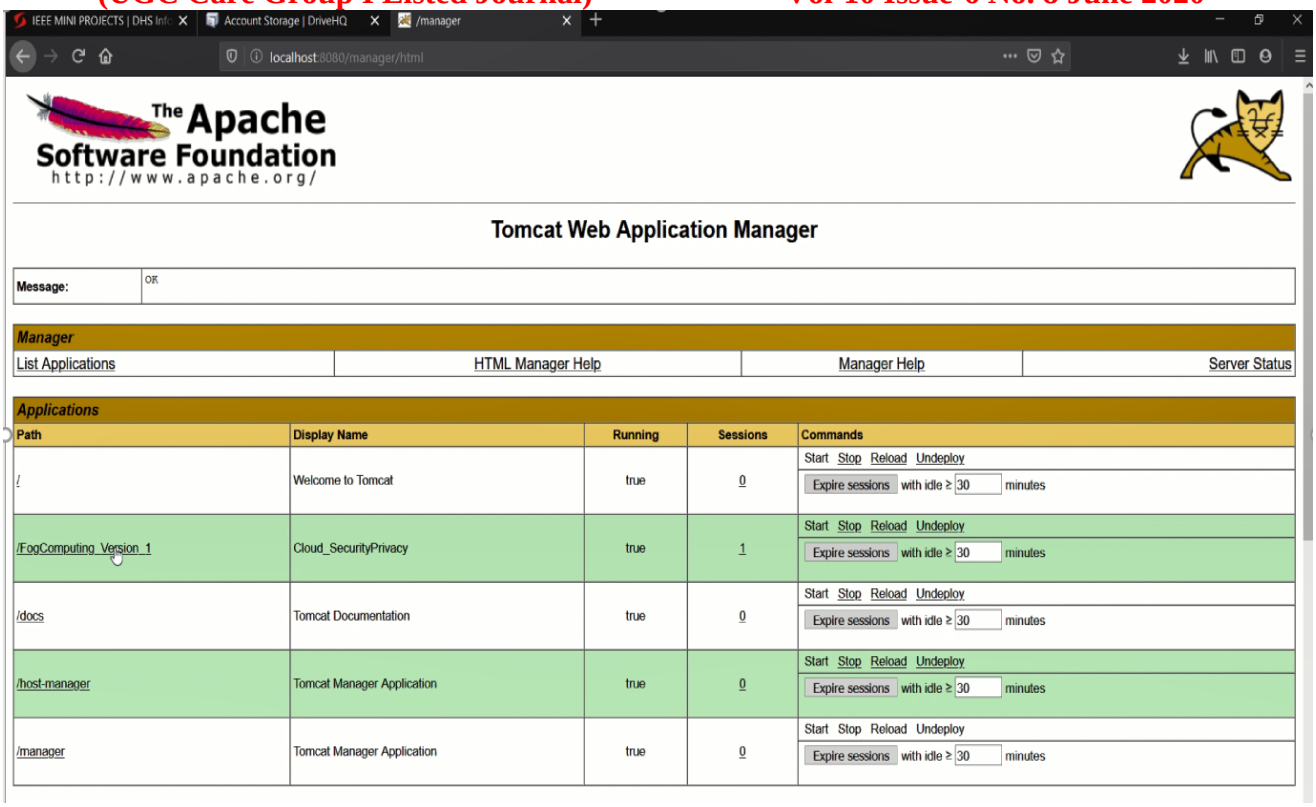


Fig 5.4 Connection of Tomcat Application Manager

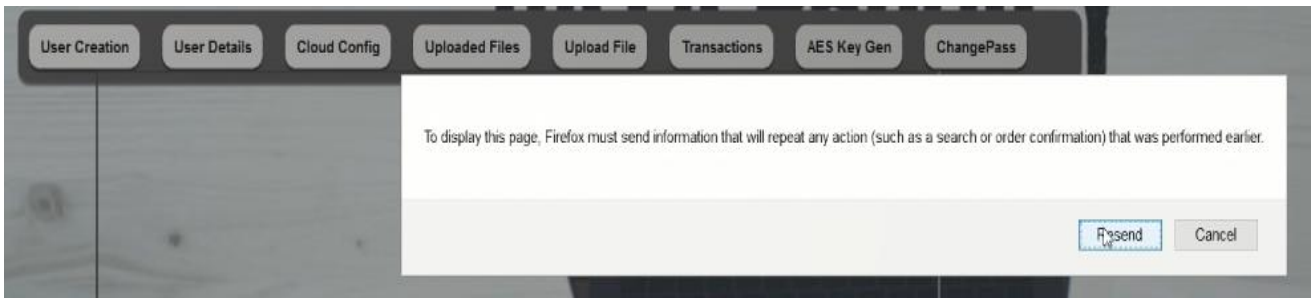
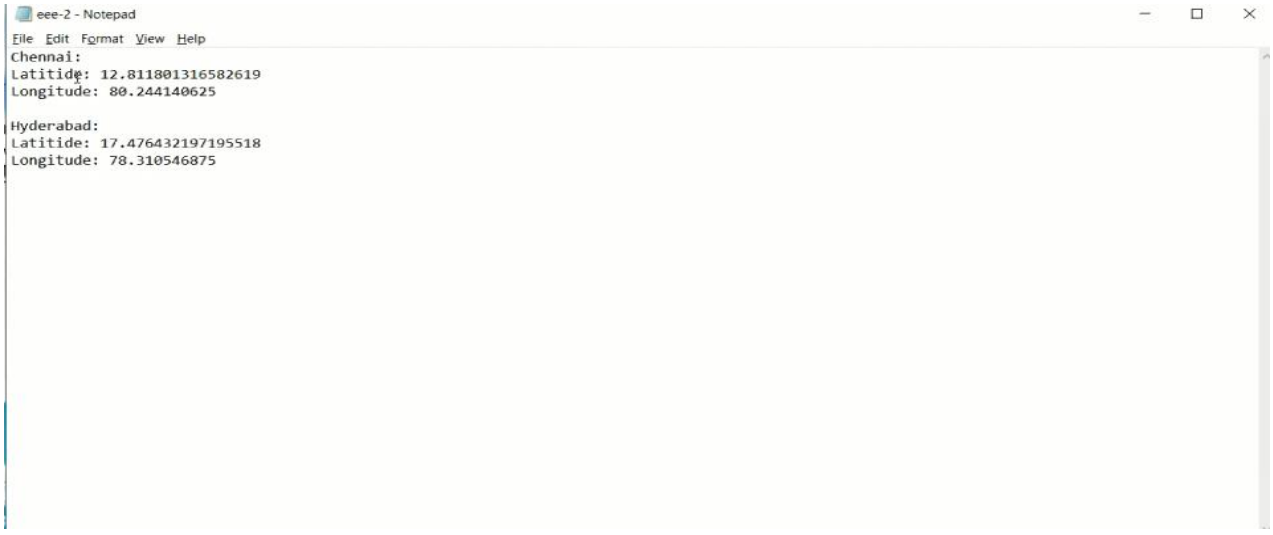


Fig 5.5 Master Key Generation and Change Password



ISSN: 2278-4632
Vol-10 Issue-6 No. 8 June 2020

Fig 5.6 Attacker achieved duplicate files

Fig 5.6 illustrates the attacker tries to gain/achieve the original files but they twice or more than that for gaining the original documents which is confidential one but instead of getting the original files the attacker gets the duplicate files.

The user creates their confidential notes and files /documents which needs to be encrypted and uploaded in the cloud service provider in which the attacker tries to gain the confidential files of authenticated user .This document is being created in notepad which makes it easy to upload in the cloud service provider.

6. CONCLUSION AND FUTURE WORK

In this system it presented a new procedure for making personal data in the cloud secure. This system had proposed supervising the data access to recognize the behavior of the user/attacker whether he/she is a malicious insider/outsider interdicted accessing the company's documents in the cloud service. So here, by developing this system in web technology, the experimental result shows this system works in proper manner.

In this approach, the future work is cloud data security becomes increasingly important as here it moves our devices, data centers, business processes, and more to the cloud.This will become most useful and safe for the users without having any tension. And the most advantage of using this solution is that no matter how much size of the document is ,this can be uploaded which will be perfectly encrypted along with message which will be received in the users email after creating the user behaviour profile. Ensuring that quality cloud data security is achieved through comprehensive security policies, an organizational culture of security, and cloud security solutions.Selecting the right cloud security solution for our business is imperative if you want to get the best from the cloud and ensure your organization is protected from unauthorized access, data breaches and other threats.

REFERENCES

[1] M. Chen, Y. Hao, K. Hwang, L. Wang and L. Wang, "Disease prediction by machine learning over big data from healthcare communities", *IEEE Access*, vol. 5, no. 1, pp. 8869-8879, 2017.

[2] M. Chen, P. Zhou and G. Fortino, "Emotion communication system", *IEEE Access*, vol. 5, pp. 326-337, 2017.

[3] M. Chen, Y. Ma, Y. Li, D. Wu, Y. Zhang and C.-H. Youn, "Wearable 2.0: Enabling human-cloud integration in next generation healthcare systems", *IEEE Commun.*, vol. 55, no. 1, pp. 54-61, Jan. 2017.

[4] S. J. Stolfo, M. B. Salem and A. D. Keromytis, "Fog computing: Mitigating insider data theft attacks in the cloud", *Proc. IEEE CS Secur. Privacy Workshops*, pp. 125-128, May 2018.

[5] "A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a fog computing Facility With Pairing-Based Cryptography", Hadeal Abdulaziz Al Hamid ; Sk Md Mizanur Rahman ; M. Shamim Hossain ; Ahmad Almogren ; Atif AlamriIEEE Access2017 Volume: 5 IEEE ACCESS.

[6] A. Alshamrani, S. Myneni, A. Chowdhary and D. Huang, "A survey on advanced persistent threats: Techniques solutions challenges and research opportunities", *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1851-1877, 2nd Quart. 2019.

[7] L. Kuang, L. Yang, J. Feng and M. Dong, "Secure tensor decomposition using fully homomorphic encryption scheme", *IEEE Trans. Cloud Comput.*, vol. 6, no. 3, pp. 868-878, 2018.

[8] J. Shen, D. Liu, Q. Liu, X. Sun and Y. Zhang, "Secure authentication in cloud big data with hierarchical attribute authorization structure", *IEEE Trans. Big Data*.

[9] D. Gonzales, J. M. Kaplan, E. Saltzman, Z. Winkelman and D. Woods, "Cloud-trust—A security assessment model for infrastructure as a service (IaaS) clouds", *IEEE Trans. Cloud Comput.*, vol. 5, pp. 523-536, Jul./Sep. 2017.

[10] C. Xu, K. Wang, P. Li, S. Guo, J. Luo, B. Ye, et al., "Making big data open in edges: A resource-efficient blockchain-based approach", *IEEE Trans. Parallel Distrib. Syst.*, vol. 30, no. 4, pp. 870-882, Apr. 2019.

[11] K. Wang, Q. Zhou, S. Guo and J. Luo, "Cluster frameworks for efficient scheduling and resource allocation in data center networks: A survey", *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3560-3580, 4th Quart. 2018.

