Survey on Preventing Data Theft in Private Cloud

M C Lavanya
Asst. Professor
NIE Collage, Mysuru, India

Kavana M D
Assistant Professor
GSSSIETW
Mysuru,India

***Abstract* - Cloud is the platform that provides us all the utilities and services as application over Internet, it is a promising technology facilitating the development of large-scale on-demand computing infrastructure. Private cloud is a cloud that will also provide entire services but it is dedicated to one particular organization. Private cloud is helpful for the business with dynamic or unpredictable computing. A private cloud provides same basic benefits of public cloud such as self service, multi-tenancy, computing resources, creating multiple machines for complex computing jobs like Big data.**

With these computing paradigms new security issues arises, which cannot be protected with the existing protection mechanism. To protect the real data we are creating a decoy file that contains some unwanted and unrelated data which will be published to the user who are not authorized to access that data. This is detected by tracking the behavior of the user while they are accessing the cloud.

I. INTRODUCTION

Cloud computing is emerged as the modern technology which developed in last few years, and considered as the next big thing, hence it has to face new security issues and challenges. the biggest challenges that companies will face as they move into the cloud environment are secure data, high speed to Internet and standardizations. Storing large amount of data in a centralized location while preserving user privacy, security, identity and their application specific preferences arises many concern about data protection. the evolution of cloud computing includes hardware, software and server virtualization

A private cloud enables data center to evolve from a fixed environment, where applications run on dedicated servers, toward an environment that is dynamic and automated, where pools of computing resources are available to support application workloads that can be accessed anywhere, anytime, from any device. Virtualization technology is fueling a significant change in today’s modern data centers, resulting in architectures that are commonly a mix of traditional and private cloud computing environments. For purposes of definition, private cloud implies that you manage the entire virtualization infrastructure. There are well known benefits of private cloud but for huge data profiles there are security issues, and data are been targeted by cyber criminals. To avoid the data being accessed by unauthorized user various encryption have been introduced, which are not so efficient with respect to cloud. Hence few new approaches such as dynamic or interactive analysis, User behavior analysis has been introduced so as to protect these data.

II. SURVEY

The security risks that threaten the network do not change when you move to the cloud. In some ways, the security risks become more significant due to the many applications on a single server premise that virtualization enables[3].

The system which we are currently working can provide only single authentication method, which is not much secure and prone to hacker. These systems does not provide any additional security features like explicitly asking to answer security questions while retrieving data. The unauthorized users can easily access the cloud and search for the files that are available. The existing system does not verify whether the user is authorized or not. The existing system provides security by encryption but it fails to secure the cloud data. Hence the Security policies must be able to monitor and keep track of the data within the cloud.

Following are various threads that is found in cloud[3]-

i. Data loss: Data loss occurs when the disk drives fails without taking any backup by the cloud owner.

ii. Denial of Services: This occurs when millions of users request the same services.

iii. Malicious insider: This occurs when a person close to us knows the login details.

iv. Shared Technology: When the information is shared by many sites the data may not be available.

v. Insecure API's: As the application programming interface are been handled by third party for verifying the user which may create threat to cloud.

One way to detect the unauthorized access is to verify the access pattern of user, if the user is genuine then he would only access the files which is of his need, where as an hacker would not have the details of the files and hence he would search various files in order to retrieve confidential data. This access patterns has to be tracked to verify the user- known as User Behavior analysis[1]. UBA tools perform two main functions. First, they determine a baseline of "normal" activities specific to the organization and its users. Second, UBA tools quickly discern deviations from that norm that require further exploration.

Once the behavior is analyzed and unauthorized user is found the real data has to be protected, this is done by flooding the user with the Decoy information[1], which is a file consist of data that are irrelevant to the real data. But for the hacker it would be the real as he will not have the details about the information stored in the file. In this way we can protect our data being accessed by the unauthorized users.

III. AUTHENTICATION

Authentication can be considered as the process of verifying the person who is claiming is the valid user. Here authentication comes with respect to the User logging onto the cloud. Every user should be introduced with a registration page which will have details of the use and authentication question. This has to be used during the file retrieval, when a user login into the cloud with the User name and password he can access the files which is related to him, during this if he wants open a file or download it then he will have to answer the security question that was given at the time of registration.

We can also implement few other security features such as explicitly entering the Aadhar card number or getting a code through OTP for the registered mobile number or E-mail id. Once this is entered the verification process starts, if the security answer matches the code of registration then the user will be provided with the real data, if the entered code does not match then the user will be flooded with the information that is not relevant to the real data hence protecting the data by unauthorized access. This is done by Decoy technology.

SMS Authentication: When the unauthorized user access the real and he will be provided with the decoy information during this the actual user has to be sent an alert message indicating the cloud data is being hacked, so that alternative security procedures can be implemented immediately so that any modifications to the data can be avoided and securing them from being accessed by hackers to misuse the confidential data.

Following is the block diagram illustrating the entire process form login till SMS authentication.

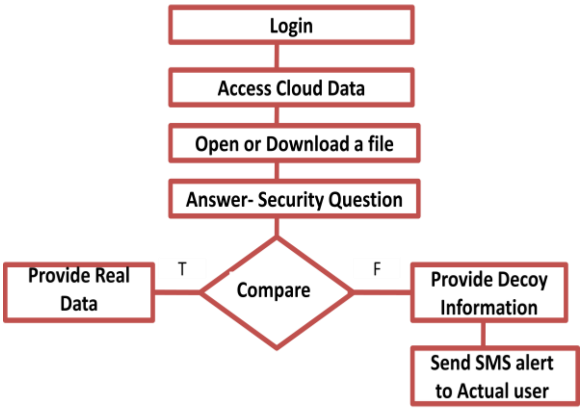
Login
Access Cloud Data
Open or Download a file
Answer- Security Question
Compare
T
Provide Real Data
F
Provide Decoy Information
Send SMS alert to Actual user

Fig: Process of Data Access

IV.CONCLUSION

This paper provide ways to protect the data stored in the cloud. This is done by tracking the user behavior and detecting the pattern in which they search the files. The user once searches any file if they want open or download it then there will be a level of protection involved- user must answer the security question, also the user must explicitly enter Aadhar card number or sending OTP to the registered mobile number or E-mail. By this the level security will be increased. If the user is unable to enter any of these then he will be flooded with the decoy information which is irrelevant to the real data. Also sends an alert message to the actual user, so that he can take necessary protection mechanism to secure the data. Hence protecting the data being misused by unauthorized users.

REFERENCES

[1] Viraj G. Mandlekar, VireshKumar Mahale, Sanket S.Sancheti, Maaz S. Rais, "Survey on Fog Computing Mitigating Data Theft Attacks in Cloud", IJIRCST, ISSN: 2347-5552, Volume-2, Issue-6, November-2014.

[2] Ali Ahmad Milad, Hjh Zaiton Muda, Zul Azri Bin Muhamad Noh, Mustafa Almahdi Algaet," Comparative Study of Performance in Cryptography Algorithms" Journal of Computer Science 8 (7): 1191-1197, 2012 ISSN 1549-3636, Malaysia, 2012.

[3] J. Pepitone, "Dropbox's password nightmare highlights cloud risks," June 2011

[4] https://www.rsa.com/en-us/products/threat detection-and-response/security-and-behavioral analytics, Networking,[accessed on 13-July-2017]

[5] https://en.wikipedia.org/wiki/User_behavior_ analytics, Wikipedia[accessed on 10-July-2017]

[6] https://www.paloaltonetworks.com/solutions/initiatives/private-cloud,Networking [accessed on 13-July-2017]

[7] John W.Rittinghouse, James F. Ransome, "Clod Computing Implementation, Management and Security", 2010 by Taylore and Francis Group, LLC, CRC Press.

[8] D. W. Chadwick and K. Fatema, "A privacy preserving authorisation system for the cloud", Journal of Computer and System Sciences, 78(5), (2012), 1359-1373.