www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-6, Issue-2, April 2018
Review Paper

Int. J. Sc. Res. in Network Security and Communication

ISSN: 2321-3256

# Attacks on Cloud Data: A Big Security Issue

**Poonam Devi**

Department of Mathematics, Chaudhary Devi Lal University, Sirsa, Haryana (India)

Received: 20/Mar/2018, Revised: 02/Apr/2018, Accepted: 18/Apr/2018, Published: 30/Apr/2018

***Abstract-*** Cloud computing is latest trend in Computing World. Every organization prefers cloud for their services, large amount of personal and professional information stored on cloud. Data theft is major security challenge on cloud because of that a person scared to us cloud for personal and professional information. Cloud Computing use various type of security like Data Security, Storage Security, and Network Security etc. But then after data theft/data hacking activities happening on cloud. If 3rd world war situations will raise then Cloud can be part of that because of these data hacking activities. Existing Technology like Encryption and password techniques are not able to prevent it. By this research paper, we want to introduce a new phase of security that is – D-Phase security with decoy technology to prevent inside data theft and to identify hacker. We can call it D- phase security with Fog computing.

***Keywords***: - Cloud Computing, Decoy, Fog computing, Security, Data theft, Identification.

## 1. INTRODUCTION

Now a day's cloud computing achieving popularity day by day, a cloud provide on demand access of resources at point of time. So every person and every organization like to use it for personal and professional work because of its ease of use, ease of communication, high storage capacity and flexibility. Because of cloud it become easy to manage data and access services at our own place but it have consequences such a data theft, and insider theft. Existing data safety mechanism such as encryption and password technique in not able to prevent data theft. Data theft is considered one of the major threats if attacker is a malicious insider, then it become more difficult to make data secure in cloud computing [1] [7]. To solve this problem we suggest a different approach for securing cloud using D-phase security with decoy technology. In D-phase we check data access in cloud, authenticate person and observe abnormal information access. When unauthorized access is assumed, system return a large amount of bogus information to that person. Our decoy information should be in same pattern as our original information so that hacker can't identify it. Securing cloud with these two phase (a) D-Phase security (b) Decoy technology will extend the use of cloud computing to its boundary level. Built a secure cloud is more important than a simple cloud. Now days we are using cloud computing in every field and organization like in financial, health and transport services etc. But if our cloud will not be secure a hacker can hack our data and can misuse it for example LAST month, Facebook revealed that over 300,000 Australians may have had their personal data accessed by political data-mining firm Cambridge Analytica. Because of less security in cloud it is not that we stop to use technology, but there is need to make it more secure.

## II. PROBLEM IN EXISTING SYSTEM

Cloud computing refer to applications and services that run on distributed networks using virtualized resources. It is a technique which provide services to clients over the network. Presently clients are using three type of Cloud services specifically Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS)[2],[8]. Where large amount of data or information of users stored on network. But nobody know where and how that data stored.

Now a day's clients are using online service like bank service where clients personal data stored on cloud, all information related to finance, business, transport, forensic and health etc. stored on cloud. It's good that we are using new technology as per growth in technology. But question rise that is it confidential? Is it secure enough as per growth in it? As per literature survey encryption method, password method or some other method of data security are not enough to make secure data on cloud, we need to use some more tool and method to make our data more secure, so that we can decrease the ratio of data theft. If our data will be more secure, clients trust on cloud will increase, more clients will use cloud services that will directly affect our country economy.

The Twitter incident is one example of a data theft attack from the Cloud. Several Twitter corporate and personal documents were ex-filtrated to technological website Tech Crunch [3], and customers' accounts, including the account of U.S. President Barack Obama, were illegally accessed. [4] The attacker used a Twitter administrator's password to gain access to Twitter's corporate documents hosted on Google's infrastructure as Google Docs.

 

De-merits of existing system

1. We can't detect when data attack happened
2. We can't detect person behind that attack.
3. We can't detect which file was hacked.

**Data Theft Record in Existing Cloud System**

As per ITRC ( Identity Theft Resource Center ) Report Jan,2016 ,Data theft ratio increases every year. The given below chart, show the cases of data theft from year 2007 to 2015[5]:

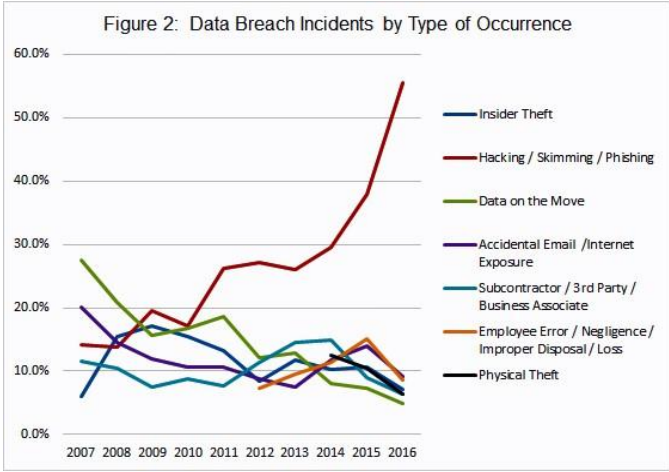


*Fig.1 Data theft Ratio in different Years*

As Show in above chart data Hacking/Phishing cases increase with very high speed as compare to other theft. If this will increase with such a speed that day will not far, that it will spread in a country like a epidemic and can destroy all resources related to cloud. If we relate it to whole world then it will work as a cyber terror and that can be a reason of 3rd world war.

## III. D-PHASE with DECOY TECHNOLOGY

In our proposed approach we want to secure data using two type of security (1) D-Phase security (2) Decoy technology, where D-Phase stands for 'Different Phase of Security'. We need D-Phase security because only decoy technology is not enough to make our data secure. In D-Phase approach we will identify behavior of user or authenticate user using D-Phase security module. We check data access in cloud, if abnormal access will found first return lot of security question and then we will return a large amount of decoy information to the user. That decoy information pattern will look like actual information that will confuse user.

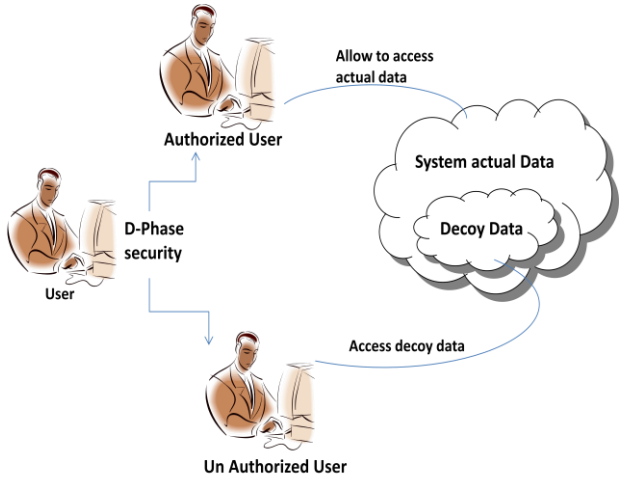


Fig. 2 Purposed system

In D-phase module of our purposed system we make system login phase more secure using OTP, Security Question and Biometric system. If a nasty person will try to access it first we trying to block him in D-Phase, but if attacker is a malicious insider then he will login into D-Phase, in that case we are checking data access in cloud, if abnormal access will found then will return large amount of security questions and after that will return bogus information to the attacker.

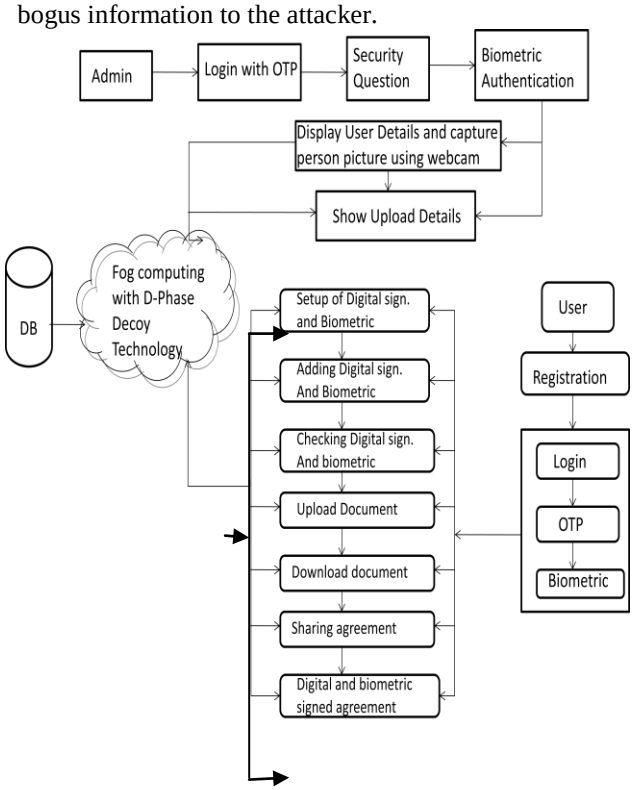


Fig. 3 System Architecture

 

## IV. SECURING CLOUD WITH D-PHASE DECOY SECURITY

Our main motive here is to make cloud more secure to decrease data theft by attackers. For that we combine D-phase security with fog computing.

### A. D-Phase Module Description:

1. Authenticate User
2. Differentiate User
3. Identify User Behavior
4. Block Nasty User

#### *1. Authenticate User*

The first phase in D-phase module is to authenticate user using login module. We have set login security as per user rights. We are using OTP, Security question and Biometric system at time of user and Admin login. OTP system will generate a unique verification code which user has to enter at time of login[2],[6]. If it is an admin login in that case after OTP it will ask security question if will give correct answer of that then it will check biometric authentication of user after that system show all details of user and will capture user picture using existing webcam.

If it is a normal user login in that case OTP Admin generates a verification code and send it to user which user has to enter at time of registration and at time of login, here admin also audit user activities, if found any abnormal access then he can block that user. We are using biometric in user login also to make user personal data more secure. For e.g. clients are using online banking services we can make it more secure using OTP and biometric.

#### 2. Differentiate User

At the time of login, login module differentiate user, whether he is normal user or Admin user and check rights of each person as per their login details. Because different user have different rights. Some have only read permission, some have both read and write permission. By using these authentications we obtain a fair and flexible control over cloud.

#### 3. Identify User Behavior

When the user will get login it is necessity to identify his behavior. Admin will control and check user behavior, he set a time line for user login and expire login session after give time period.[7] He monitor data access on cloud like which file user try to access and how often and if notice any abnormal access he can block the user. But if the attacker is an insider in that case we suggest a different security level that is face recognition after login. If system finds some mismatch then return decoy information to user. Some time service providers can be an attacker in that case it is difficult to identify attacker but we can confuse him using decoy technique.

#### 4. Block Nasty User

If we find any nasty person from user profile behavior system directly block him using D-Phase security[1], [8]. If attacker is an insider then system ask security question, capture a picture of attacker using webcam to identify him and block that client..

### *B. Confuse Attackers with Decoy Technology*

Using Decoy Technology in fog computing, we want to secure our cloud, in which we will confuse the attacker by placing trap files (that are fake files appearing real to the attacker) in the users file system.[2],[8] If attacker enters the system, he will open the files to which access is open, if he do random search then system audit his action and return a large amount of bogus information followed by security questions.

ADVANTAGES-

- Detection of masquerade activities.
- Confuse attacker using bogus information.

DISADVANTAGES-

- Nobody is identified when the attack was happen.
- We can't detect which file was hacked.

## V. CONCLUSION

The malicious attacks causes cloud computing security. In this paper we present two phase security to make our cloud secure, where in first D-Phase we authenticate user profile behavior and prevent him from data access if navigational patterns are recorded. In second phase – decoy technology allow the user to access bogus or decoy information in the file system to misguide insider data theft attacker. Once unauthorized data access is suspected, system verified it with lot of challenging questions and return decoy information in the file system.

## REFERENCES


[1]. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6227695

[2]. http://docplayer.net/6393704-Defining-the-cloud-battlefield.html

[3]. M. Arrington, "In our inbox: Hundreds of con- fidential twitter documents," July 2009. [Online]. Available: http://techcrunch.com/2009/07/14/in-our-inbox-hundreds-ofconfidential-twitter-documents

[4]. D. Takahashi, "French hacker who leaked Twitter documents to TechCrunch is busted," March 2010. [Online]. Available: http://venturebeat.com/2010/03/24/french-hacker-wholeaked-twitter-documents-to-techcrunch-is-busted/

[5]. http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html

[6]. D.C.Saste,P.V.Madhwai,N.B.Lokhande and V.N.Chothe FOG COMPUTING: Comprehensive Approach for Avoiding Data Theft Attack Using Decoy Technology


 

[7]. http://ijsae.in/ijsaeems/index.php/ijsae/article/view/697
[8] .Cloud Security Alliance, "Top Threat to Cloud Computing V1.0," March 2010. [Online]. Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

 