FOG COMPUTING: A NEW CONCEPT TO MINIMIZE THE ATTACKS AND TO PROVIDE SECURITY IN CLOUD COMPUTING ENVIRONMENT

Sonali Khairnar[1], Dhanashree Borkar[2]

[1]*M.E, Department of CSE, JSPM's Imperial college of Engineering and Research, Maharashtra, India*
[2]*B.E, Department of CSE, JSPM's Imperial college of Engineering and Research, Maharashtra, India*

Abstract

Cloud is basically a clusters of multiple dedicated servers attached within a network .Cloud Computing is a network based environment that focuses on sharing computations or resources. In cloud customers only pay for what they use and have not to pay for local resources which they need such as storage or infrastructure. so this is the main advantage of cloud computing and main reason for gaining popularity in todays world .Also cloud computing is one of the most exciting technology due to its ability to reduce cost associated with computing while increasing flexibility and scalability for computer processes .But in cloud the main problem that occurs is security .And now a days security and privacy both are main concern that needed to be considered. To overcome the problem of security we are introducing the new technique which is called as Fog Computing .Fog Computing is not a replacement of cloud it is just extends the cloud computing by providing security in the cloud environment. With Fog services we are able to enhance the cloud experience by isolating users data that need to live on the edge. The main aim of fog computing is to place the data close to the end user.

Keywords: *Cloud, Cloud Computing, Decoys, Fog Computing.*

----------***----------

1. INTRODUCTION

In today's worlds the small as well as big -big organizations are using cloud computing technology to protect their data and to use the cloud resources as and when they need . Cloud is a subscription based service .Cloud computing is a shared pool of resources. The way of use computers and store our personal and business information can arises new data security challenges. Encryption mechanisms not protect the data in the cloud from unauthorized access. As we know that the traditional database system are usually deployed in closed environment where user can access the system only through a restricted network or internet. With the fast growth of W.W.W user can access virtually any database for which they have proper access right from anywhere in the world . By registering into cloud the users are ready to get the resources from cloud providers and the organization can access their data from anywhere and at any time when they need. But this comfortness comes with certain type of risk like security and privacy. To overcome by this problem we are using a new technique called as fog computing. Fog computing provides security in cloud environment in a greater extend to get the benefit of this technique a user need to get registered with the fog. once the user is ready by filling up the sign up form he will get the msg or email that he is ready to take the services from fog computing.

1.1 Existing System

Existing data protection mechanisms such as encryption was failed in securing the data from the attackers. It does not verify whether the user was authorized or not. Cloud computing security does not focus on ways of secure the data from unauthorized access. Encryption does not provide much security to our data. In 2009 We have our own confidential documents in the cloud. This files does not have much security. So, hacker gains access the documents. Twitter incident is one example of a data theft attack in the Cloud. Difficult to find the attacker. In 2010 and 2011 Cloud computing security was developed against attackers. Finding of hackers in the cloud. Additionally, it shows that recent research results that might be useful to protect data in the cloud.

1.2 Proposed System

We proposed a completely new technique to secure user's data in cloud using user behavior and decoy information technology called as Fog Computing. We use this techniques to provide data security in the cloud . A different approach for securing data in the cloud using offensive decoy technology. We monitor data access in the cloud and detect abnormal data access patterns. In this technique when the unauthorized person try to access the data of the real user the system generates the fake documents in such a way that the unauthorized person was also not able to identify that the data is fake or real .It is identified thought a question which is entered by the real user at the time of filling the sign up form. If the answer of the question is wrong it means the user is not the real user and the system provide the fake document else original documents will be provided by the system to the real user.

2. SECURING CLOUDS USING FOG

There are various ways to use cloud services to save or store files, documents and media in remote services that can be accessed whenever user connect to the Internet. The main problem in cloud is to maintain security for users data in way that guarantees only authenticated users and no one else gain access to that data. The issue of providing security to confidential information is core security problem, that it does not provide level of assurance most people desire. There are various methods to secure remote data in cloud using standard access control and encryption methods. It is good to say that all the standard approaches used for providing security have been demonstrated to fail from time to time for a variety of reasons, including faulty implementations, buggy code, insider attacks, mis-configured services, and the creative construction of effective and sophisticated attacks not envisioned by the implementers of security procedures. Building a secure and trustworthy cloud computing environment is not enough, because attacks on data continue to happen, and when they do, and information gets lost, there is no way to get it back. There is needs to get solutions to such accidents. The basic idea is that we can limit the damage of stolen data if we decrease the value of that stolen data to the attacker. We can achieve this through a 'preventive' decoy (disinformation) attack. We can secure Cloud services by implementing given additional security features.

2.1 Decoy System

Decoy data, such as decoy documents, honeypots and other bogus information can be generated on demand and used for detecting unauthorized access to information and to 'poison' the thief's ex-filtrated information. Serving decoys will confuse an attacker into believing they have ex-filtrated useful information, when they have not. This technology may be integrated with user behavior profiling technology to secure a user's data in the Cloud. . Whenever abnormal and unauthorized access to a cloud service is noticed, decoy information may be returned by the Cloud and delivered in such a waythat it appear completely normal and legitimate. The legitimate user, who is the owner of the information, would readily identify when decoy information is being returned by the Cloud, and hence could alter the Cloud's responses through a variety of means, such as challenge questions, to inform the Cloud security system that it has incorrectly detected an unauthorized access. In the case where the access is correctly identified as an unauthorized access, the Cloud security system would deliver unbounded amounts of bogus information to the attacker, thus securing the user's true data from can be implemented by given two additional security features: (1) validating whether data access is authorized when abnormal information access is detected, and (2) confusing the attacker with bogus information that is by providing decoy documents.

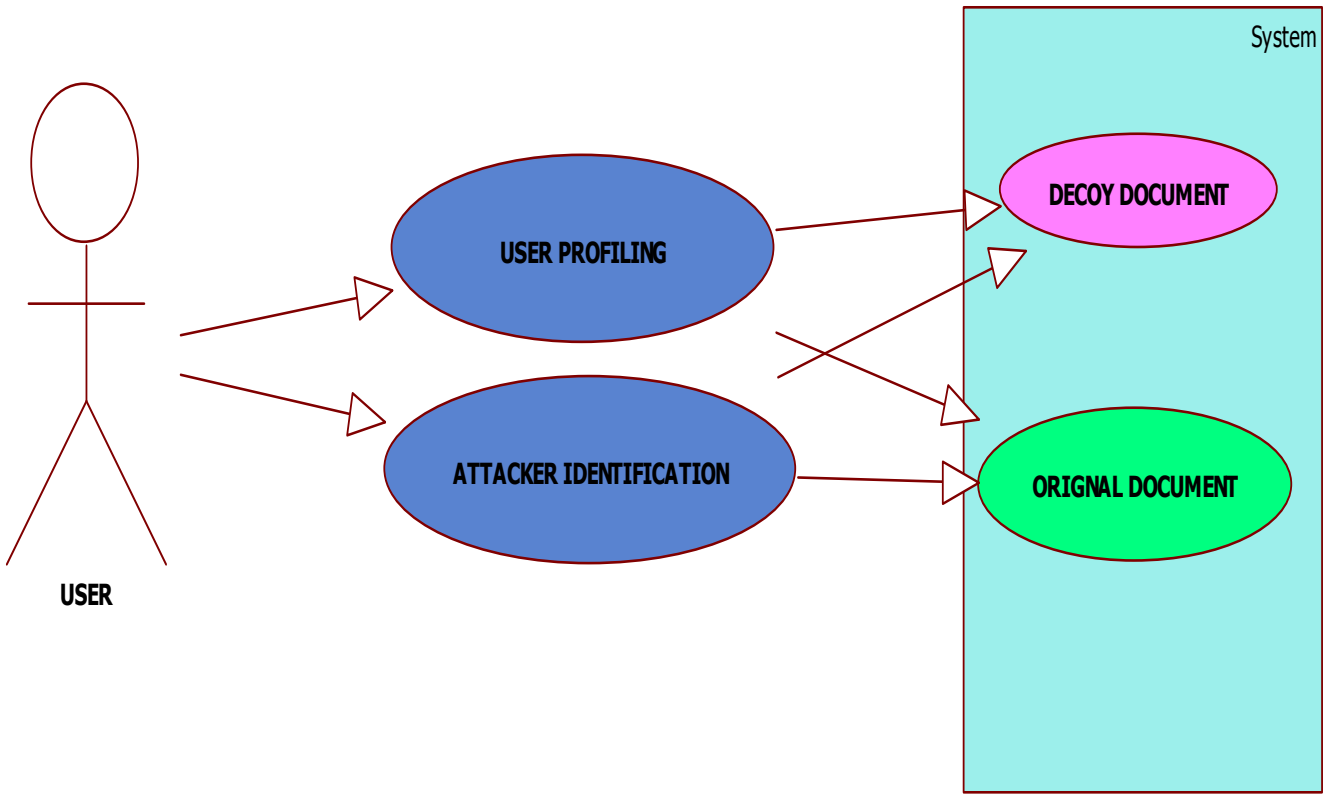

Fig -1: Decoy System

We have applied above concepts to detect unauthorized data access to data stored on a local file system by masqueraders, i.e. attackers who view of legitimate users after stealing their credentials. Our experimental results in a local file system setting show that combining both techniques can yield better detection results .This results suggest that this approach may work in a Cloud environment, to make cloud system more transparent to the user as a local file system.

3. FOG COMPUTING

Fog Computing system is trying to work against the attacker specially malicious insider. Here malicious insider means Insider attacks can be performed by malicious employees at the providers or users site. Malicious insider can access the confidential data of cloud users. A malicious insider can easily obtain passwords, cryptographic keys and files. The threat of malicious attacks has increased due to lack of transparency in cloud providers processes and procedures . It means that a provider may not know how employees are granted access and how this access is monitored or how reports as well as policy compliances are analyzed.

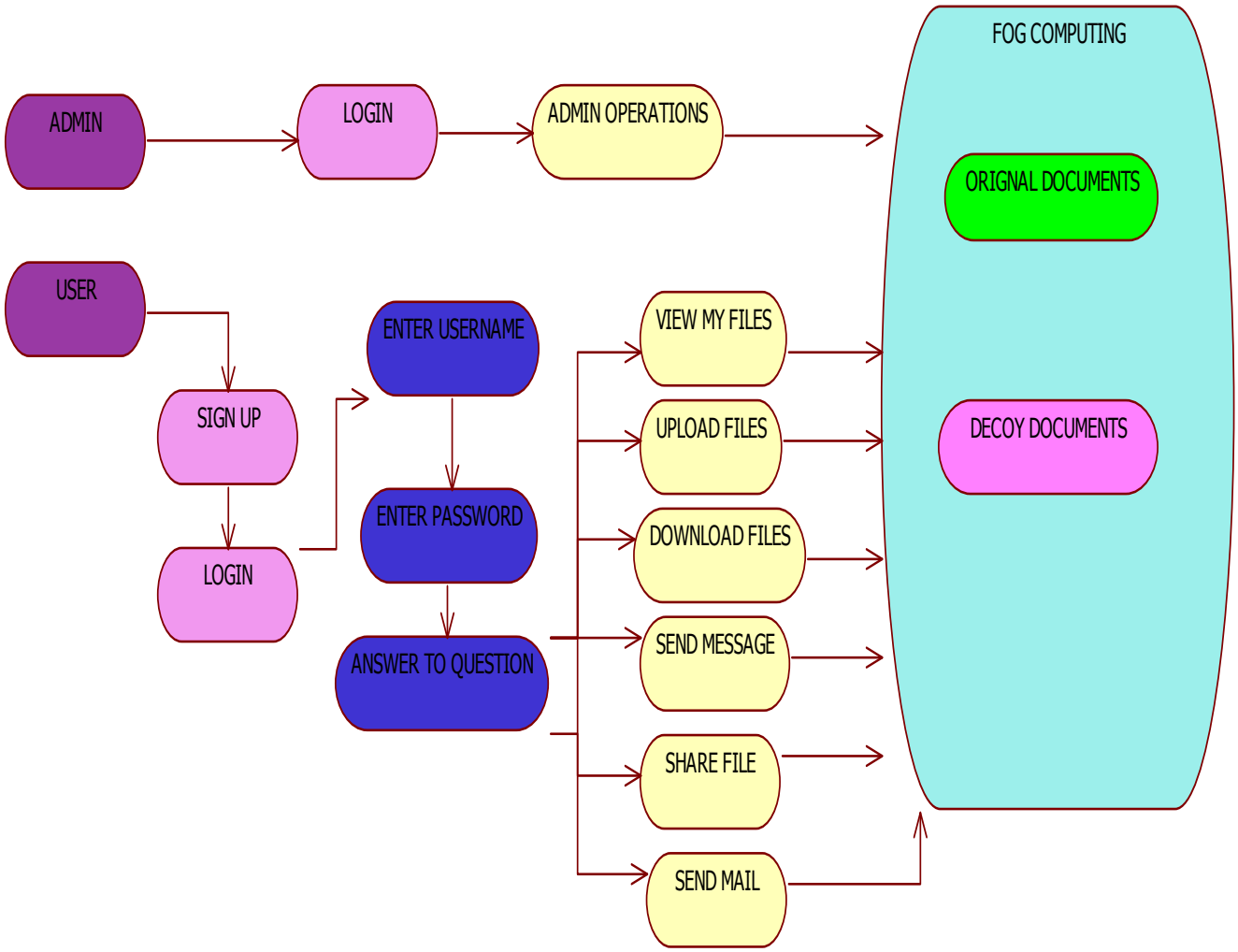

Fig -2: Architecture of Fog Computing

Above fig. states the actual working of the fog computing .In two ways login is done in system that are admin login and user login .When admin login to the system there are again two steps to follow: step1:Enter username step2:Enter the password . After successful login of admin he can perform all admin related tasks, but while downloading any file from fog he have to answer the security Question if he answer it correctly then only original file can be download.
In other case ,when admin or user answer incorrectly to the security question then decoy document (fake document) is provided to the fake user . Decoy technology work in the given manner if you have any word ,suppose “MADAM” in the document then some alphabets are replaced as M->A then the given word become “AADAA” which have no meaning. In some Case ,if attacker getting to know that ‘M’ is replaced by ‘A’ in the given document and by applying reverse engineering he get result as “MMDMM”. In any case he can’t judge content of document.

When user login to the system he also have to follow the same procedure as admin. Operations like upload files/documents, download files/documents, view alerts, send message, read message, broadcast any message all these can be perform by the user. ALERT this stream provide the detail knowledge of attack done on their personal file/document with details like date, time, no of times the attacker trying to hack that file/document .Best thing of fog Computing is after each successful login the user get SMS on the mobile that 'login successful'. from this the user get alert when other else trying to gain access to his/her personal fog account and when attacker trying to download some files/documents then user also get SMS that contain attacker ip-address, attacker's server name, date, time details on his/her mobile so that become easy to catch attacker by tracing all these things.

In this way fog computing is more secure than the traditional cloud computing.

4. CONCLUSIONS

The system was developed only with email provision but we have also implemented the SMS technique. In Fog Computing we presenting a new approach for solving the problem of insider data theft attacks in a cloud using dynamically generated decoy files and also saving storage required for maintaining decoy files in the cloud. So by using decoy technique in Fog can minimize insider attacks in cloud.

REFERENCES

[1]. Cloud Computing for Dummies
[2]. Prevention Of Malicious Insider In The Cloud Using Decoy Documents by S. Muqtyar Ahmed, P. Namratha, C. Nagesh
[3]. Cloud Security: Attacks and Current Defenses Gehana Booth, Andrew Soknacki, and Anil Somayaji
[4]. Overview of Attacks on Cloud Computing by Ajey Singh, Dr. Maneesh Shrivastava

BIOGRAPHIES

Sonali Khairnar is lecturer of JSPM's Imperial College of Engineering and Research, Pune, MH, INDIA. She has received M.E Degree Computer Science and Engineering, Her main research interest includes Cloud Computing, Databases.

Dhanashree Borkar is Student of JSPM's Imperial College of Engineering and Research, Pune, MH, INDIA. Currently appeared for B.E Degree Computer Science and Engineering, Her main research interest includes Cloud Computing and Fog Computing.