DOI 10.4010/2016.634
ISSN 2321 3361 © 2016 IJESC

Research Article Volume 6 Issue No. 3

FOG Computing

Jayshree Khandagale[1], Deepak Fodse[2], Poonam Sul[3], Prita Patil[4]
Department of Computer Engineering
Mumbai University, Vidyalankar Institute of Technology, Mumbai, India.
Jayshreekhandagale12@gmail.com[1], fodse.deepak143@gmail.com[2], poonamsul30@gmail.com[3], prita.patil@gmail.com[4]

Abstract:
Nowadays huge amount of data is stored on cloud. Cloud computing promises to significantly change the way we use computers and access and store our personal and business information. Because of these new computing and communication paradigm there arise data security challenges. In this paper, we proposed a system for securing data stored in the cloud using decoy technology. In this we monitor data access in the cloud and detect abnormal data access. When unauthorised access is detected that users activity will be tracked in log details table. Based on the activities performed by unauthorized user admin can blocked or delete that user. When a new user enters into this System, he have to register first. After successfully registered, that user will get a key through mail. And during login, if the user enter wrong password continuously more than three times, he will get access and his activity will be tracked on log details table in the database. (that is in the action column trialpwd will be entered).And after this , whatever activities he is doing that also will be tracked in the log table .If he downloads any file, he won't get original file. Instead of that he will get decoy file. If a user entered correct password and he will get access .If that user wants to download any file, and he entered wrong key more than three times, in first three cases in the action column invalid will be entered and in the fourth case wrong key and that user will get decoy file .In every case it Now will execute user behaviour algorithm. When a user edit password he enters wrong key more than three times , then edit pwd wrong key will be entered. And user will get message that password updated successfully. But in actual case it is not updating.

Keywords: decoy files, access control.

I. INTRODUCTION

Cloud computing is achieving popularity and gaining attention in business organizations. It offers a variety of services to the users. It is an ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources [1]. Due this ease, software companies and other agencies are shifting more towards cloud computing environment. To achieve better operational efficiency in many organizations and small or medium agencies is using Cloud environment for managing their data. Cloud Computing is a combination of a number of computing strategies and concepts such as Service Oriented Architecture (SOA), virtualization and other which rely on the Internet. It is considered as a delivery platform in which resources are provided as a service to the client through the Internet. Although, Cloud Computing provides an easy way for accessing, managing and computation of user data, but it also has some severe security risks. There are some traditional security mechanism such as identity, authorization and authentication, but now these are not sufficient [2]. Fog computing, also known as fogging, is a model in which data, processing and applications are concentrated in devices at the network edge rather than existing almost entirely in the cloud. Cloud computing promises to significantly change the way we use computers and access and store our personal and business information. Because of these new computing and communication paradigm there arise data security challenges. Even though existing techniques use security mechanisms, data theft attacks prevention fails. To overcome this we can use decoy technology to secure data stored in cloud.

It works in the following manner:-

1) We monitor data access in the cloud and detect abnormal data access patterns. When unauthorized access is suspected and then verified using challenge questions.

2) We launch a disinformation attack by returning large amount of decoy information to the attacker. This protects against the misuse of the user's real data

II. LITERATURE REVIEW

The present system provides only the single authentication which is not much secure and can easily be hacked by a hacker. The system does not provide any additional security like security questions for more security. The hacker can easily get into the cloud and search for the files that are available. The present 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

Threats in cloud:

1. Data breaches – This led to the loss of personal data and credit card information of about 110 million people, it was one of the theft during processing and storage of data.
2. Data loss – Data loss occurs when the disk drive dies without any backup created by the cloud owner. It occurs when the encrypted key is unavailable with the owner.
3. Account or service traffic hijacking – Account can be hacked if the login credentials are lost.
4. Insecure API's – Application Programming Interface controls the third party and verifies the user.
5. Denial of service – This occurs when millions of user request of same service and the hackers take this .
6. Malicious insiders – This occurs when a person close to us knows our login credentials.
7. Abuse of cloud services – By using many cloud servers hacker can crack the encryption in very less time.
8. Insufficient due diligence- Without knowing the advantages and disadvantages of the cloud many businesses and firms jump into cloud thus leading to data loss.

9. Shared technology – This occurs when the information is shared by the many sites.

III. PROPOSEDWORK

We propose a distinct approach to secure cloud known as Fog Computing.

•We use decoy information and user behaviour profiling to secure data on Cloud.

•The proposed mechanism facilitates security features to data and thereby allows for detection of invalid access

•It provides prevention to enable valid distribution of data.

Methodology

There are two main modules:

User:

User can have the following functionalities:

1. login
2. Edit password
3. Upload files
4. View files and Download
5. Search files
6. Key Recovery.

Admin:

Admin can have the following functionalities:

1. Upload decoy-Admin can upload decoy files
2. Manage files
3. Manage users-Can block and delete user based on the activities.
4. User logs-Maintains log details of all users

Modules:

1. User Authentication: The user is facilitated here to authenticate and thus, ensure that only valid users can access the application. But, it also tracks the user login operation and accordingly redirects the user to the decoy application.

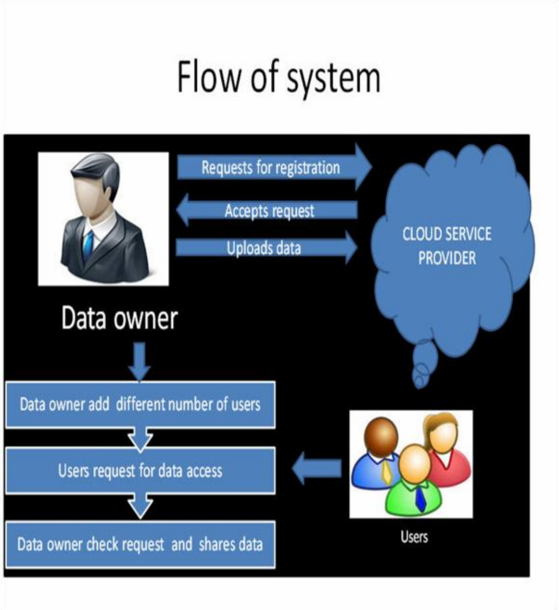
2. Admin Module: This module facilitates the admin to manage users, the data stored and the invalid activities occurring within the application. Thus, this user will be responsible for tracking the application functionalities. A set of valid access rules will also be defined by the admin for identification of invalid users.

3. File Access Module: This module will enable to track whether the search operations executed by the user follow a valid set of operations or not. Accordingly, the system will decide whether the user should be redirected to the decoy environment.

4. Data Access Module: The data available for user access will be authenticated using a separate user key specified by the application to the user during registration. Based on the validity of this user key the system will redirect the user to the Decoy Module for tracking and prevent invalid distribution of data.

5. Decoy Module: This module will facilitate the system to redirect invalid users to a dummy set of modules wherein invalid data will be distributed to the invalid user and the user activities will be notified to the admin. Thus, the system will not notify the invalid user about the detection of invalid activity and prevent

IV. IMPLEMENTATION AND ANALYSIS


Flow of system
Requests for registration
Accepts request
Uploads data
CLOUD SERVICE PROVIDER
Data owner
Data owner add different number of users
Users request for data access
Data owner check request and shares data
Users

When a new user enters into this System he has to register first. After successfully registration that user will get a key through mail.

•And during login if the user enter wrong password continuously more than three times he will get access and his activity will be tracked on log details table in the database And after this whatever activities he is doing that also will be tracked in the log table .If he downloads any file he won't get original file Instead of that he will get decoy file.

•If a user enters correct password he will get access .If that user wants to download any file and he enters a wrong key more than three times .In first three cases, invalid entries will be entered in the action column .In the fourth case if wrong key is entered then that user will get decoy file .In every case it will execute user behaviour algorithm.

•When a user edit password he enters wrong key more than three times, then editpwdwrong key will be entered and user will get message that password updated successfully. But in actual case it is not updating.

User behaviour Algorithm:

```
It will take user id as input.
1) Set  THREASH = 0.5f;
 COUNT = 4, MIN_RECORDS = 5;
2) In an Array List we will Store Some actions.
l.add("wrong key");
l.add("invalid");
l.add("trialkey");
l.add("decoy");
l.add("editpwdwrongkey");
l.add("editpwdtrialkey");
l.add("wrongpwd");
l.add("trialpwd");
3) Takes number of rows in the log details table for that user.
4) If the number of rows less than minimum records, returns validate.
5) Else
Set invalid=0.
```

Takes action from the log details of that user, if it contain any operation mentioned in the array list invalid count will be incremented.

6) It will calculate

Set value=0, row=0

Value = value + (((float) invalid) / ((float) COUNT));

7) find avg = (number of rows for that user in log details tab / 2)

if value>=THREASH, increments row.

8) This will repeat for all rows .If rows > avg, returns invalid date. else returns validate. In short, User behaviour algorithm returns the behaviour of That particular user based on the entries in log details table. if this returns invalidate then in the action column decoy will be entered. Suppose If the user entered correct password and he got access. At the time of downloading he entered correct key. Then User behaviour algorithm will execute. It will take number of invalid entries in the table and returns either validate or invalidate. If its return invalidate then during downloading he will get decoy file even if that user enter correct key. In every case this algorithm will execute. At the time of key recovery it will be verified using challenging questions.

Admin

Admin can have the following functionalities,

1. Upload decoy-Admin can upload decoy files
2. Manage files-
3. Manage users-Can block and delete user based on the activities.
4. User logs-Maintains log details of all users

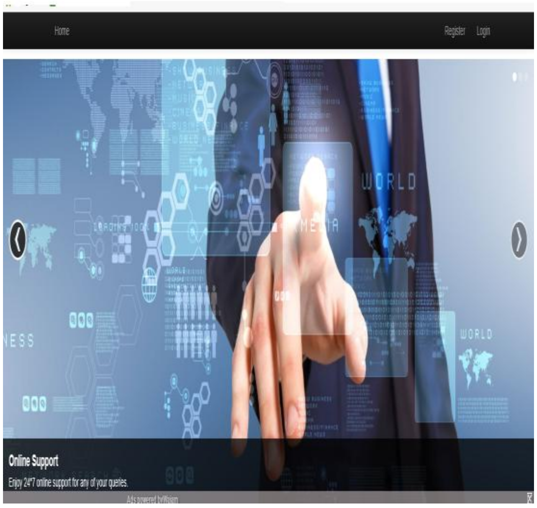
Process Model Used for the Project

A spiral model of software development and enhancement. This model is the iterative model which is used in implementation of this project. Each phase starts with a design goal and ends with a client reviewing the progress thus far project, with an eye toward the end goal of the project.

The steps for Spiral Model can be generalized as follows:

- The new system requirements are defined in as much details as possible. This usually involves interviewing a number of users representing all the external or internal users and other aspects of the existing system.
    - A preliminary design is created for the new system.
    - A first prototype of the new system is constructed from the preliminary design. This is usually a scaled-down system, and represents an approximation of the characteristics of the final product.
    - A second prototype is evolved by a fourfold procedure:
        1. Evaluating the first prototype in terms of its strengths, weakness, and risks.
        2. Defining the requirements of the second prototype.
        3. Planning a designing the second prototype.
        4. Constructing and testing the second prototype.
- At the customer option, the entire project can be aborted if the risk is deemed too great. Risk factors might involve development cost overruns, operating-cost miscalculation, or any other factor that could, in the customer's judgment, result in a less-than-satisfactory final product.
- The existing prototype is evaluated in the same manner as was the previous prototype, and if necessary, another prototype is developed from it according to the fourfold procedure outlined above.
- The preceding steps are iterated until the customer is satisfied that the refined prototype represents the final product desired.
- The final system is constructed, based on the refined prototype.
- The final system is thoroughly evaluated and tested. Routine maintenance is carried on a continuing basis to prevent large scale failures and to minimize down time.

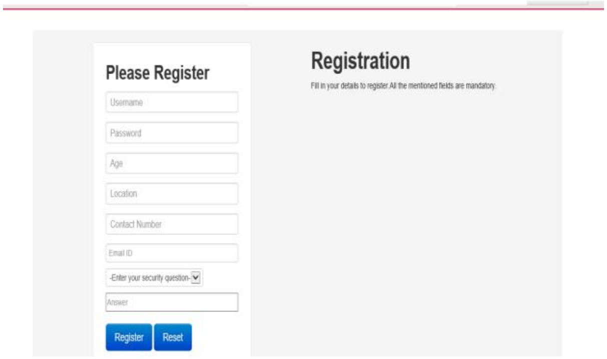
V. EXPERIMENTAL RESULTS AND DISCUSSION



Online Support

Enjoy 24*7 online support for any of your queries.

Fig 1: User Interface

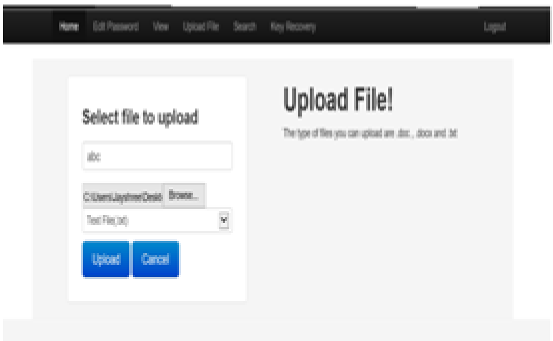


Please Register

Registration

Fill in your details to register.All the mentioned fields are mandatory.

Fig 2: Registration Form



Select file to upload

abc

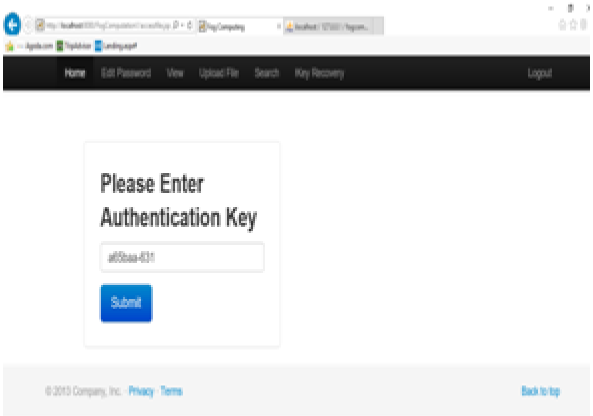
C:\Users\Jayshree\Desk Browse...

Text File(.txt)

Upload File!

The type of files you can upload are .doc, .docx and .txt

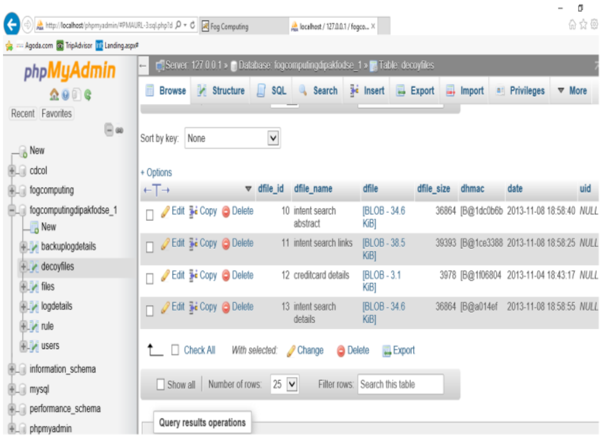
Fig 3: File Upload



Please Enter Authentication Key

a65baa-631

Fig 4: Download File



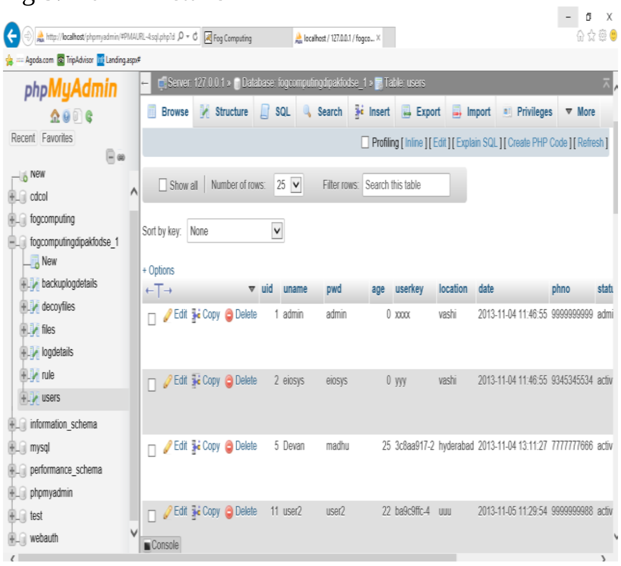
Server: 127.0.0.1 » Database: fogcomputingdipakfodse_1 » Table: decoyfiles

Sort by key: None

	dfile_id	dfile_name	dfile	dfile_size	dhmac	date	uid
□ Edit Copy Delete	10	intent search abstract	[BLOB - 34.6 KiB]	36864	[B@1dc0b6b	2013-11-08 18:58:40	NULL
□ Edit Copy Delete	11	intent search links	[BLOB - 38.5 KiB]	39393	[B@1ce3388	2013-11-08 18:58:25	NULL
□ Edit Copy Delete	12	creditcard details	[BLOB - 3.1 KiB]	3978	[B@1f06804	2013-11-04 18:43:17	NULL
□ Edit Copy Delete	13	intent search details	[BLOB - 34.6 KiB]	36864	[B@a014ef	2013-11-08 18:58:55	NULL

□ Show all | Number of rows: 25 | Filter rows: Search this table

Fig 5: Admin Details



Server: 127.0.0.1 » Database: fogcomputingdipakfodse_1 » Table: users

□ Show all | Number of rows: 25 | Filter rows: Search this table

Sort by key: None

	uid	uname	pwd	age	userkey	location	date	phno	statu
□ Edit Copy Delete	1	admin	admin	0	xxxx	vashi	2013-11-04 11:46:55	9999999999	admi
□ Edit Copy Delete	2	eiosys	eiosys	0	yyy	vashi	2013-11-04 11:46:55	9345345534	activ
□ Edit Copy Delete	5	Devan	madhu	25	3c8aa917-2	hyderabad	2013-11-04 13:11:27	7777777666	activ
□ Edit Copy Delete	11	user2	user2	22	ba9c9ffc-4	uuu	2013-11-05 11:29:54	9999999988	activ

Fig 6: User Details

VI. CONCLUSION

We present an approach for securing business data in the cloud. Once unauthorised access or exposure is suspected, and later verified, with challenge questions for that instance, then we inundate the malicious insider with bogus information in order to dilute the user’s real data.

VII. REFERENCES

[1] Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud, USA

[2] Ben-Salem M., and Stolfo Angelos D. Keromytis, “Fog computing: Mitigating Insider Data Theft Attacks in the Cloud,” IEEE symposium on security and privacy workshop (SPW) 2012.

[3] Ben-Salem M., and Stolfo, “Decoy Document Deployment for Effective Masquerade Attack Detection,” Computer Science Department, Columbia University, New York.

[4] F. Bonomi, "Connected vehicles, the internet of things, and fog computing," in The Eighth ACM International Workshop on Vehicular Inter-Networking (VANET), Las Vegas, USA, 2011.

[5] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, ser. MCC'12. ACM, 2012, pp. 13-16.

[6] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50-58, Apr 2010.

[7] C. Wei, Z. Fadlullah, N. Kato, and I. Stojmenovic, "On optimally reducing power loss in micro-grids with power storage devices," IEEE Journal of Selected Areas in Communications, 2014 to appear.

[8] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Comput. Netw., vol. 54, no. 15, pp. 2787-2805, Oct. 2010.

[9] K. Liu, J. Ng, V. Lee, S. Son, and I. Stojmenovic, "Cooperative data dissemination in hybrid vehicular networks: Vanet as a software defined network," Submitted for publication, 2014.

[10] K. Kirkpatrick, "Software-defined networking," Commun. ACM, vol. 56, no. 9, pp. 16-19, Sep. 2013.

[11] Cisco, "Cisco delivers vision of fog computing to accelerate value from billions of connected devices," Cisco, Tech. Rep., Jan. 2014.

[12] K. Hong, D. Lillethun, U. Ramachandran, B. Ottenw¿¡lder, and B. Koldehofe, "Opportunistic spatio-temporal event processing for mobile situation awareness," in Proceedings of the 7th ACM International Conference on

Distributed Event-based Systems, ser. DEBS'13. ACM, 2013, pp. 195-206.

[13] H. Madsen, G. Albeanu, B. Burtschy, and F. Popentiu-Vladicescu, "Reliability in the utility computing era: Towards reliable fog computing," in Systems, Signals and Image Processing (IWSSIP), 2013 20th International Conference on, July 2013, pp. 43-46.

[14] K. Hong, D. Lillethun, U. Ramachandran, B. Ottenw lder, and B. Koldehofe, "Mobile fog: A programming model for large-scale applications on the internet of things," in Proceedings of the Second ACM SIGCOMM Workshop on Mobile Cloud Computing, ser. MCC'13. ACM, 2013, pp. 15-20.