International Journal of Trend in Research and Development, Volume 2(2), ISSN: 2394-9333
www.ijtrd.com

Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud

Ashvini Machale[1] , Hemlata Mulay[2],Varsha Taware[3],Virendrakumar Dhotre[4]

[1,2,3,4]Savitribai Phule Pune University,
H.S.B.P.V.T.COE, Kashti, Shrigonda - 414701, Ahemednagar.

Abstract: We propose a completely different approach to securing the cloud using auto log-out, that we have come to call Fog computing. This option is being configured by us: to use the auto-logout against fake users who try to get the data. The function of auto-log out, serves two purposes: (1) validating whether data access is authorized when abnormal information access is detected, and (2) confusing the attacker by logging then out from the system. The customers who use the cloud only pay for what they use and have not to pay for local resources which they need such as infra or storage. This acts as the main benefit and the main reason for gaining popularity in today's world. In order to overcome the issue of security we are introducing the new technique which is called as Fog Computing . This does not replace the cloud as a system, it just extends the cloud computing by providing security in the cloud environment. With Fog services we are able to improvise the cloud experience by isolating users data that is important. The main objective of the fog computing is to place the data close to the user.

Keywords: Cloud, Cloud Computing, Fog Computing Security, Auto-logout Technology.

1. Introduction

Businesses, especially small and medium businesses (SMBs), start-ups etc are going in for data outsourcing and cloud-computation. This really enables for better operational efficiency, however incurs greater risks, perhaps the most serious of which are data theft attack. Theft attacks of data are greatly high if the attacker is a harmful insider. CSA (Cloud Security Alliance) takes this to be one of the major threats. Most people who are on cloud computing are well-aware of this threat, they have no other option but to trust the service provider when it comes to protecting their data. The reduced amount of transparency into, very less control over, the Cloud provider's authorization, audit controls, and authentication only makes this threat worse. Hence we thought of a completely different approach to securing the cloud using auto-logout information technology, that is being called as Fog computing. This technology to launch auto-logout attacks against harmful users, preventing .them from getting access to the actual data.

In this paper, we propose two ways of using Fog computing to prevent attacks such as the Twitter attack, by deploying auto-logout information within the Cloud by the Cloud service customer and within personal online social networking profiles by individual users.

2. Literature Survey

The way we access our computers and the way we store our information pertaining to personal and business would change significantly is a promise that cloud computing makes. With these types of new measures (communications and computing) coming into picture there is a challenge that comes up with regards to the data security. When we have an insider to the provider of the cloud as the harmful user, the existing protection methods like encryption fails to protect the data. Much research in Cloud computing security has focused on ways of preventing unjustified and illegitimate access to data by developing encryption mechanisms and sophisticated access control. But these measures have not been able to prevent data compromise.

3. Securing cloud using Fog

There are various ways to use cloud services to save or store media, files, documents etc in remote services that can be accessed whenever user connect to the Internet. The main problem in cloud is to ascertain security for user's data in way that guarantees only authenticated users and no one else gain access to that information. The problem of providing safety to confidential/secret information is core security issue, it does not provide a level of assurance that most people desire. Various methods are present to ensure the security of remote data in cloud using the standard access control, encryption methods etc. However it can be said that all the standard approaches used for assuring security have failed from time to time for a number of reasons, which includes buggy code, insider attacks, faulty implementations, mis-configured services, and the creative implementation of effective and sophisticated attacks not thought of by the people who implement the security procedures. Building a secure and trustworthy cloud computing environment does not solve this issue, because data attacks continue to happen, in addition to that when they happen, and information gets lost/corrupt, we fail on getting that back. There has to be a solution to these types of accidents. The fundamental idea is to limit the damage that can be caused due to stolen data, if we do not allow access to the data to the intruder. This can be achieved through a preventive auto-logout attack. Providing additional features to secure the data will help cloud computing.

3.1. User Behavior Profiling

Data access in the cloud is being monitored by us and the abnormal access patterns for the data is being detected by us. User profiling is a well known Technique that can be applied

here to know who, when, and how a person accesses their information in the Cloud. Such 'ordinary user' behavior can be continuously checked to determine whether abnormal access to a user's information is happening. Fraud revelation software normally uses these types of behaviour based security measures. These types of profiles would by default include information on how many docs are read and that too how often. The system monitors for search behaviours that are abnormal and display deviations from the user baseline. The combination of search behavior patterns along with trap-based auto-logout of the user should provide stronger evidence of failures, and therefore improve a systems accuracy.

4. Fog Computing

Fog Computing system is trying to work against the attacker specially harmful user. Here harmful user means Insider attacks can be performed by harmful employees at the providers or users site. Harmful user can access the confidential data of cloud users. A harmful user can easily obtain passwords, encoded keys and files. The threat of harmful attacks has increased due to lack of transparency in cloud providers processes and procedures. The provider of the service 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-1.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 document is not provided to the fake user .

In any case he will auto logout. 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 all these can be perform by the user. ALERT this stream provide the detail knowledge of like date, time, no of times Best attack done on their personal file/document with details the attacker trying to hack that file/document. Thing of fog Computing, get Mail on the E-Mail-id. 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 Mail that contain attacker ipaddress, attackers server name, date, time details on his/her mobile so that become easy to catch attacker by tracing all these things. This helps fog-computing to be more secure than the traditional cloud computing

5. Cloud insider attack revelation

The Fog Computing Validation requires

System 1: Test Web Application

a) The application should be deployed on a cloud server. b) The Application is used to test and to validate the Fog Computing System revelation. The Test We Applications are the basic inputs for Fog Computing. Every application should provide the following: Store user name, password, confirm password and at least one secrete questions at the time of account creation.

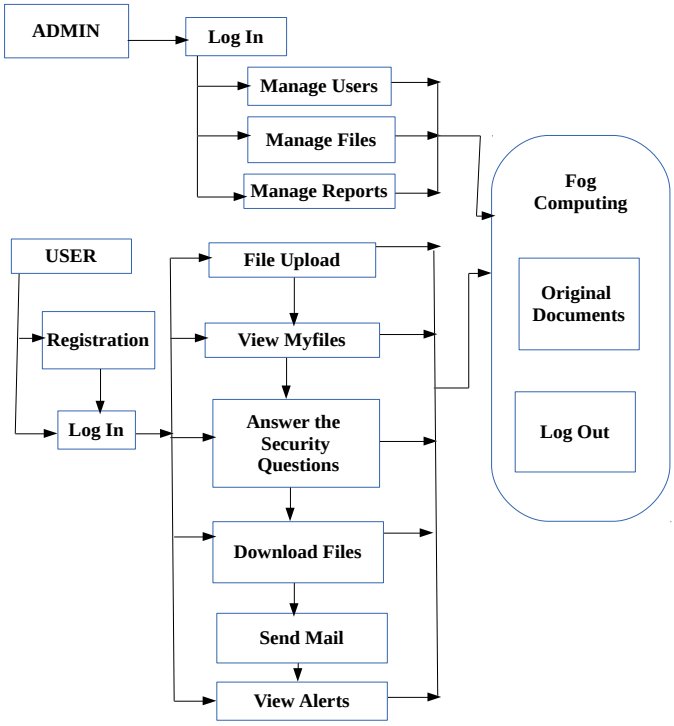


Fig -1: Architecture of Fog Computing

System 2: Fog Computing System

a)To profile or store the user access behavior .b) It analyzes the present behavior with the past profile. The system has an interface to view the un-expected user accesses. It provides logs of un-expected revelation system. 1.User Access Behavior Profiling. 2.File System Maintenance. 3.un-expected revelation. 4.Security Question. 5.View Alerts.

1. User Access Behavior Profiling:

The module is concerned about storing the use's request to files on the web application. The system's module keeps track of how many files were read and how often. The operations include create, read, delete ,etc.

2. File System Maintenance:

For each newly created folder or a file, corresponding file will be maintained.. Means that newly uploaded file is stored in specified folder. These all uploaded and downloaded files are maintained by the Administrator. The directory and file structure is same for the original file system.

3. un-expected revelation:

The current logged in user access behavior is compared with the past behavior of the user. If the behaviour of the user is exceeding the value which is set up as a threshold or a limit, then the remote user is suspected to be un-expected. If the current user behavior is as the past behavior, then the user will be able to work on the data which is original.

4. Security Question:

If the current user's behavior seems un-expectedious, then the user is asked for randomly selected secret questions. If the user is not able to provide correct responses for a certain limits, the user is not provided with files. If the user provided correct answers for a limit, the user is treated as ordinary user.

5. View Alerts.
When unjustified person is detected then view alerts are updated randomly.

System 3: Administration System
The system is an interface to view the un-expected unjustified user accesses. It allows the admins to administrate allow/reject policies for the remote users. It provides logs of un-expected revelation system.

6. Algorithm

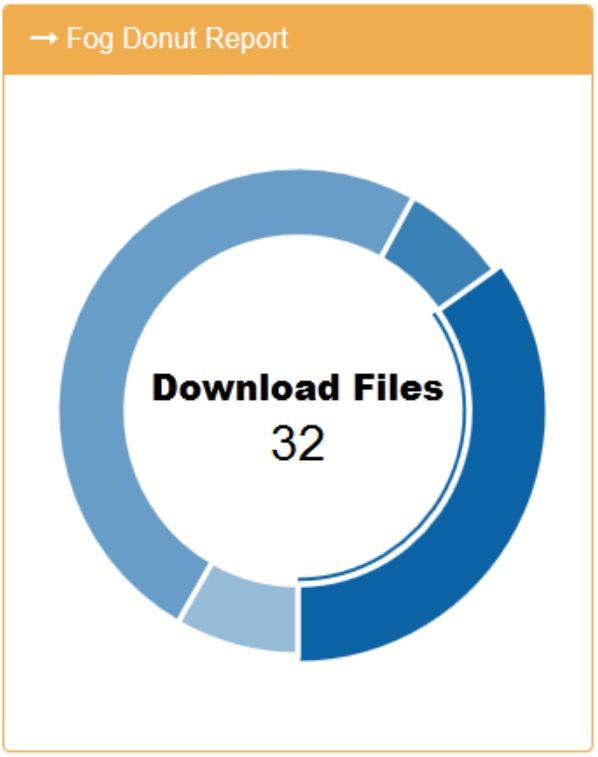
There are 2 types of users for the system; namely:
1. Admin
2. Ordinary user

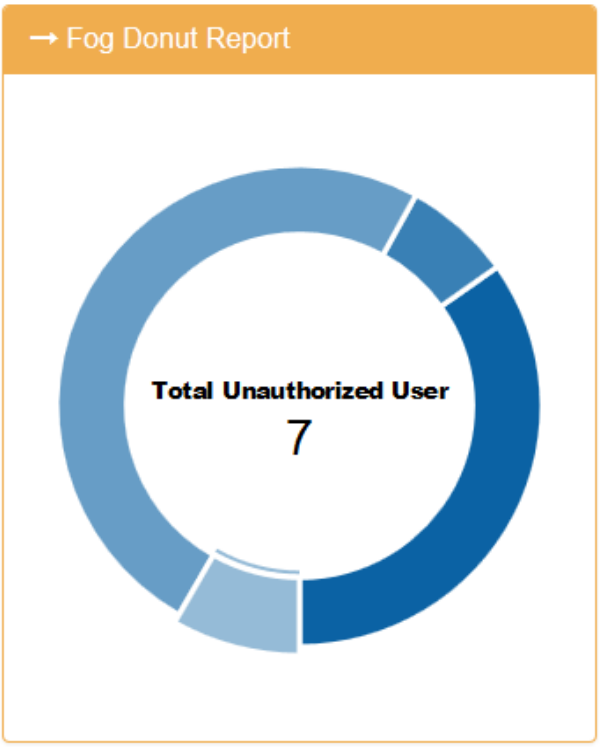
1. As an admin, the user will be able to perform the below:
a. Login to the system.
b. Once the admin logs in they would be presented with 2 options viz:
b1. Manage the users who have signed up and also get the stats for their activities.
b2. Manage the files that are being uploaded by the users

2. As a ordinary user, they would be able to perform the below:
a. Register to the system
a1. The registration will have the ordinary fields that are required viz: The email address, password etc. However there is a secret question option which is a mandatory option. This question would be asked whenever the user is downloading a file from the system. If the answer is wrong then the user will not be able to download + they would also be logged out of the system
b. Login to the system
c. The logged in user will be able to perform the below actions:
c1. File upload:
c1.i. From this page the user will be able to upload a file from their pc to the system. While they are uploading, they can also provide a name for the file that could be given to it. This is the velationname of the file that would be displayed in the files manager.
c2. View My Files
c2.i. Using this option the user gets a clear idea of the file that they have uploaded.
c2.ii. They can click on it and download the same too back to the pc that they are user
c2.iii. However to perform the above step there is a security question that needs to be answered to validate the user again.
c2.iv. On this screen there are 2 columns that displays the downloads that are done for the file as well as the alerts for unsuccessful downloads.
c3. Answer the security question
c3.i. This can be termed as a two step validation in the system.
c3.ii. When the user is trying to download any file from the system, he / she needs to answer the security question that was added by them in the system during registration.
c3.iii. If the users fail to do so then the file download will fail as well as they would be logged out of the system.

7. Reports

There are 2 reports that are being provided:
1. Fog donut report
1a. This report displays the total number of users, total number of unjustified users, downloaded files, total files that are present in the system.

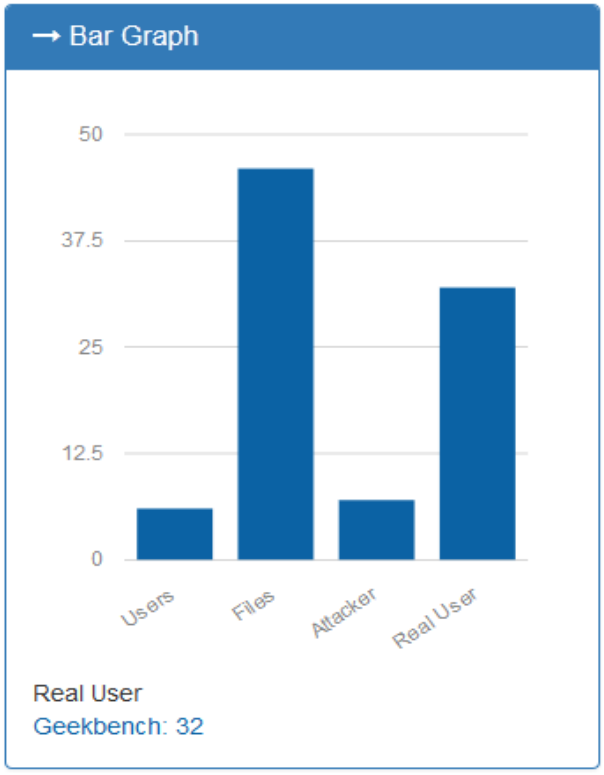


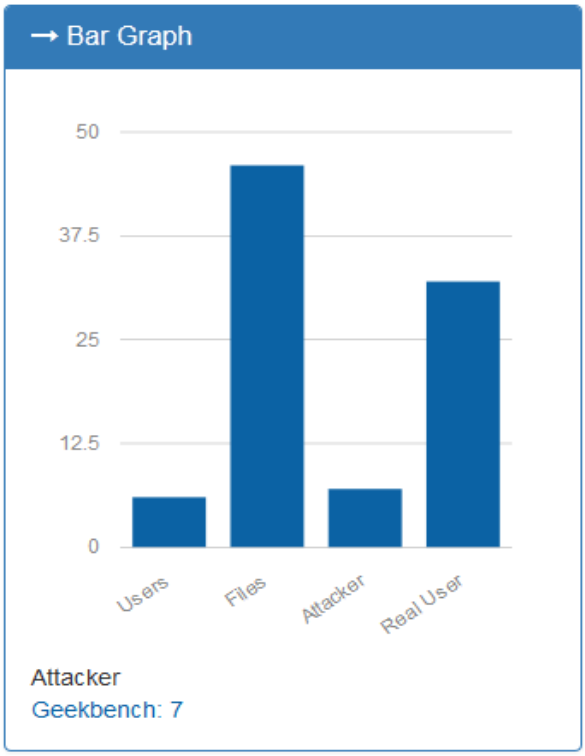


2. Bar graph
2a. This is the aggregator report for the system.

2b. This displays the number of users, files, attackers and real users by the system

2c. The type of component is displayed in the x axis and the y axis is being broken down into numbers which are in multiples of 10.





8. Future Work

Each and every users behaviour is being tracked and a user behaviour profile is being maintained. This would help in understanding and making the systems algorithms better with regards to the tracking of the attackers and the attacks. Even the study would be done of the attacks and the attackers by keeping a track of their behaviour too, this would further be analyzed in depth. Data can also be split-up and saved / stored on multiple platforms for providing enhanced security.

Conclusion

We present a novel approach to securing personal and business data in the Cloud. We conclude that data monitoring access patterns by profiling user behavior to determine if and when a harmful user illegitimately accesses someone's documents in a Cloud service. Auto-logout of the system in the Cloud alongside the real data of the users also serve as sensors to detect illegitimate access. When we suspect unjustified data access or exposure, and later verify the same, with the tactical question for instance, we inundate the harmful user by logging them out of the system in order to confuse the attackers and protect the data present in the system. Preventive attacks such as this that rely on auto-logout technology ,could provide enhanced security levels in the Cloud and in social networks.

REFERENCES

[1] A salya and Ravi M, "survey on defense against insider misuse attacks in the cloud", in Proceedings of the international journals of advanced computing ,2013.

[2] S. J. Stolfo, M. B. Salem and A. D. Keromytis, "Fog computing: Mitigating insider data theft attacks in the cloud", in Proceedings of the IEEE Symposium on Security and Privacy workshop, 2012.

[3] J. A. Iglesias, P. Angelov, A. Ledezma, and A. Sanchis, "Creating evolving user behavior profiles automatically," IEEE Trans. on Knowl. and Data Eng. May 2012.

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

[5] M. Ben-Salem and S. J. Stolfo, "Modeling user search-behavior for masquerade detection," in Proceedings of the 14th International Symposium on Recent Advances in Intrusion Detection. Heidelberg: Springer, September 2011.

[6] M. Ben-Salem and S. J. Stolfo, "Combining a baiting and a user search profiling techniques for masquerade detection," in Columbia University Computer Science Department, Technical Report # cucs-018-11, 2011.

[7] R.L.Krutz and R.D.Vines, —Cloud Computing Software Security Fundamentals in Cloud Security: A Comprehensive Guide to Secure Cloud Computing, New York City, NY, Wiley, 2010.

[8] B. M. Bowen and S. Hershkop, "Decoy Document Distributor" 2009.

[9] M. Arrington, "In our inbox: Hundreds of confidential twitter documents," July 2009.

[10] D. Godoy, "User profiling for web page filtering," IEEE Internet Computing,Jul. 2005.