www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume – 5 Issue -03 March, 2016 Page No. 16009-16012

Fog Computing: Securing the cloud and preventing insider attacks in the cloud.

Aatish B. Shah[1], Jai Kannan[2], Deep Utkal Shah[3] Prof. S.B.Ware[4], Prof. R.S.Badodekar[5]
[1][2][3]Department of Information Technology
[1][2][3]Sinhgad Institute of Technology, Lonavala
1aatish333@gmail.com
2jones.kannan17@live.com
3deepushah04@gmail.com

Abstract: ***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. Although, Fog Computing is defined as the extension of the Cloud Computing paradigm, its distinctive characteristics in the location sensitivity, wireless connectivity, and geographical accessibility create new security and forensics issues and challenges which have not been well studied in Cloud security and Cloud forensics.***
We monitor data access in the cloud and detect abnormal data access patterns. When unauthorized access is suspected and then verified using challenge questions, we launch a disinformation attack by returning large amounts of decoy information to the attacker. This protects against the misuse of the user's real data. Experiments conducted in a local file setting provide evidence that this approach may provide unprecedented levels of user data security in a Cloud environment.

Keywords: Cloud Computing, Decoy System, Data Security, Fog Computing.

1. INTRODUCTION

CISCO recently delivered the vision of fog computing to enable applications on billions of connected devices, already connected in the Internet of Things (IoT). IoT combines information and computing processes to control very large collections of different objects. [1]

In today's world the small as well as large organizations are using cloud computing technology to protect their data and to use the cloud resources as and when they need. The existing mechanisms only facilitate security features to data and thereby don't allow for detection of invalid access and thereby its prevention to enable valid distribution of data. The proposed mechanism facilitates security features to data and thereby allows for detection of invalid access and thereby its prevention to enable valid distribution of data. Data theft attacks are amplified if the attacker is a malicious insider. This is considered as one of the top threats to cloud computing by the Cloud Security Alliance. While most Cloud computing customers are well-aware of this threat, they are left only with trusting the service provider when it comes to protecting their data. The lack of transparency into, let alone control over, the Cloud provider's authentication, authorization, and audit controls only exacerbates this threat. Fog Computing provides security to the data stored in the cloud. This helps the users to be tension free about the security of their data. If any unauthorized user tries to access the data in the cloud, then the security will track the user and will map all the data concerned with the user. We use this technology to launch disinformation attacks against malicious insiders, preventing them from distinguishing the real sensitive customer data from fake worthless data. [2]

2. LITERATURE SURVEY

In July 2009, Michael Arrington published a paper with the topic "In our inbox: Hundreds of confidential twitter documents". The guy ("Hacker Croll") who claims to have accessed hundreds of confidential corporate and personal documents of Twitter and Twitter employees, is releasing those documents publicly and sent them to us earlier today. The zip file contained 310 documents, ranging from executive meeting notes, partner agreements and financial projections to the meal preferences, calendars and phone logs of various Twitter employees. There is clearly an ethical line here that we don't want to cross, and the vast majority of these documents aren't going to be published, at least by us. But a few of the documents have so much news value that we think it's appropriate to publish them.

Then in March 2010, Muhammad Kazim University of Derby, United Kingdom Shao Ying Zhu University of Derby, United Kingdom, published a paper on the topic "Cloud Security Alliance, "Top Threat to Cloud Computing V1.0". According to this paper, cloud computing offers many advantages such as increased utilization of hardware resources, scalability, reduced costs, and easy deployment. As a result, all the major companies including Microsoft, Google and Amazon are using cloud computing. Moreover, the number of customers moving their data to cloud services such as iCloud, Google Drive, Dropbox, Facebook and LinkedIn are increasing every day.

2.2 RELATED WORK DONE

a) Ulteo Cloud:

The vision is to enable organizations to connect their employees with the applications and information they need to be successful. By transforming the way applications and desktops are delivered and accessed we help streamline IT delivery while enabling new ways of working. Ulteo is a commercial open source vendor, our customers benefit from the ethos of the open source model with the security and backing of a commercial enterprise. Our mission is to deliver non-proprietary platforms built on innovation, independence and an open architecture. Ulteo offers the most cost efficient application delivery platform to the market today, with Ulteo OVD Community Edition (free to use) and Ulteo Premium Edition giving administrators the ability to seamlessly deliver applications or full desktop sessions to PCs, Macs, tablets, smart phones, laptops and thin clients from Windows, Linux and cloud environments.[3]

b) Wargaming.net:

Wargaming Public Co Ltd is an international game developer and publisher. The developed a MMO in 2012 with the name World of Tanks. This MMO is a server based game which requires the players to create a personal account and then they can play. The game consists of many skills which are complex to handle. There are also various scripts which can be executed while playing the game which simplifies the game. These scripts work like hacks for the players and they can easily spam their opponents. To avoid the players from doing this, Wargaming released a patch in which the players using various scripts to hack the game were reported by the players and their accounts would get deactivated.

3. SECURING CLOUDS WITH FOG:

Numerous proposals for cloud-based services describe methods to store documents, files, and media in a remote service that may be accessed wherever a user may connect to the Internet. A particularly vexing problem before such services are broadly accepted concerns guarantees for securing a user's data in a manner where that guarantees only the user and no one else can gain access to that data. The problem of providing security of confidential information remains a core security problem that, to date, has not provided the levels of assurance most people desire. Many proposals have been made to secure remote data in the Cloud using encryption and standard access controls.

It is fair to say all of the standard approaches have been demonstrated to fail from time to time for a variety of reasons, including insider attacks, mis-configured services, faulty implementations, buggy code, and the creative construction of effective and sophisticated attacks not envisioned by the implementers of security procedures. Building a trustworthy cloud computing environment is not enough, because accidents continue to happen, and when they do, and information gets lost, there is no way to get it back. One needs to prepare for such accidents. The basic idea is that we can limit the damage of stolen data if we decrease the value of that stolen information to the attacker. We can achieve this through a 'preventive' disinformation attack. [4]

We posit that secure Cloud services can be implemented given two additional security features:

1. User Behavior Profiling:

It is expected that access to a user's information in the Cloud will exhibit a normal means of access. User profiling is a well known technique that can be applied here to model how, when, and how much a user accesses their information in the Cloud. Such 'normal user' behavior can be continuously checked to determine whether abnormal access to a user's information is occurring. This method of behavior-based security is commonly used in fraud detection applications. Such profiles would naturally include volumetric information, how many documents are typically read and how often. These simple user specific features can serve to detect abnormal Cloud access based partially upon the scale and scope of data transferred.

2. Decoys:

Decoy information, such as decoy documents, honeypots, and various other bogus information can be generated on demand and serve as a means of detecting unauthorized access to information and to 'poison' the thief's ex-filtrated information. Serving decoys will confound and confuse an adversary 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 information in the Cloud. Whenever abnormal access to a cloud service is noticed, decoy information may be returned by the Cloud and delivered in such a way as to appear completely legitimate and normal. The true 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 inaccurately 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 adversary, thus securing the user's true data from unauthorized disclosure. The decoys, then, serve two purposes:

(A) Validating whether data access is authorized when abnormal information access is detected.

(B) Confusing the attacker with bogus information. We posit that the combination of these two security features will provide unprecedented levels of security for the Cloud. No current Cloud security mechanism is available that provides this level of security. We have applied these concepts to detect illegitimate data access to data stored on a local file system by masqueraders, i.e. attackers who impersonate legitimate users after stealing their credentials. One may consider illegitimate access to Cloud data by a rogue insider as the malicious act of a masquerader. Our experimental results in a local file system

setting show that combining both techniques can yield better detection results, and our results suggest that this approach may work in a Cloud environment, as the Cloud is intended to be as transparent to the user as a local file system. In the following we review briefly some of the experimental results achieved by using this approach to detect masquerade activity in a local file setting.

4. WHAT IS TO BE DEVELOPED

Cloud computing promises to significantly change the way we use computers and access and store our personal and business information. With these new computing and communications paradigms arise new data security challenges. Existing data protection mechanisms such as encryption have failed in preventing data theft attacks, especially those perpetrated by an insider to the cloud provider. We propose 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. When unauthorized access is suspected and then verified using challenge questions, we launch a disinformation attack by returning large amounts of decoy information to the attacker. This protects against the misuse of the user's real data. Experiments conducted in a local file setting provide evidence that this approach may provide unprecedented levels of user data security in a Cloud environment. This is 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 unauthorized access is detected, that users activity will be tracked in log details table.

4.1 MODULES:

a) 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.

b) 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.

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

d) 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.

e) 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 further attack on the system. The decoy data stored will be differentiated by the system using HMAC tag attached to the data.

5. DESIGN

5.1 SYSTEM ARCHITECTURE:

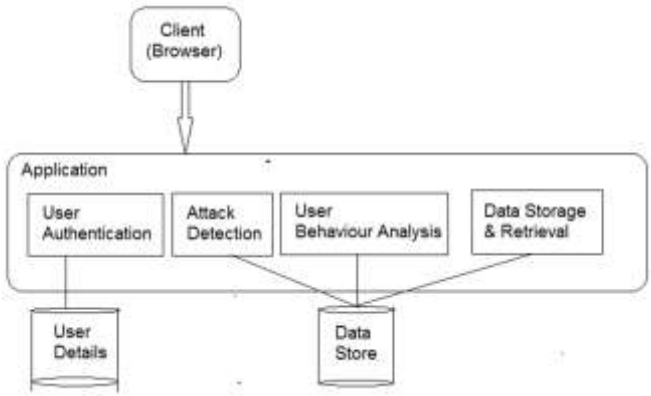

Figure 1: System Architecture

6. ALGORITHM:

User Behavior Profiling Algorithm:

1. Identify operation executed.
2. Track user behavior profile consisting of the following parameters: username, login password specified, user key specified during document access, type of document selected for access (valid or decoy).
3. During login, login password specified is tracked
4. During document access, the user key specified is tracked along with the type of operation (valid or invalid).
5. Classify profile as valid or invalid using the following analyzed using the following mathematical operation: P(IV)=count(invalid operations of each type)/count(operations of each type). If the value P (IV) is above a threshold parameter then the profile is categorized as invalid and the user is redirected to the decoy module.

7. ACKNOWLEDGEMENT:

We the students of SINHGAD INSTITUTE OF TECHNOLOGY,LONAVALA (BRANCH – IT), are extremely grateful for the confidence bestowed in me and & my fellow colleagues entrusting our project entitled "FOG COMPUTING". At this juncture I feel deeply honored in

expressing my sincere thanks to Mr. Navid Nalband (Project Manager) for making the resources available at right time and providing valuable insights leading to the successful completion of my project. I also extend my gratitude to my Project Guide Prof. S. B. Ware, who assisted me in compiling the project. I would also like to thank all the faculty members of Sinhgad Institute of Technology, Lonavala (Branch – IT) for their critical advice and guidance without which this project would not have been possible. Last but not the least I place a deep sense of gratitude to my family members and my friends who have been constant source of inspiration during the preparation of this project work and technical paper.

8. CONCLUSION:

We present a novel approach to securing personal and business data in the Cloud. We propose monitoring data access patterns by profiling user behavior to determine if and when a malicious insider illegitimately accesses someone's documents in a Cloud service. Decoy documents stored in the Cloud alongside the user's real data also serve as sensors to detect illegitimate access. Once unauthorized data access or exposure is suspected, and later verified, with challenge questions for instance, we inundate the malicious insider with bogus information in order to dilute the user's real data. Such preventive attacks that rely on disinformation technology could provide unprecedented levels of security in the Cloud and in social networks.

9. REFERENCES:

[1] Clinton Dsouza Gail-Joon Ahn Marthony Taguinod, "Policy-Driven Security Management for Fog Computing:PreliminaryFrameworkandACaseStudy," Laboratory of Security Engineering for Future Computing (SEFCOM) School of Computing, Informatics, and Decision Systems Engineering Arizona State University. *IEEE IRI 2014, August 13-15, 2014*

[2] Ryoichi Sasaki and Tetsutaro Uehara, Fog Computing: Issues and Challenges in Security and Forensics, Cambridge University Press, Cambridge, *1982. 0730-3157/15© 2015 IEEE.*

[3] Cloud Security Alliance, "Top Threat to Cloud Computing V1.0," March 2010. *[Online]*.

[4] 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, pp. 1–20.*

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

[6] William Y Chang, Hosame Abu-amara, Jessica Stanford, "Transforming enterprise cloud services" (Book Form).

10. AUTHOR PROFILE

Aatish B. Shah
*Pursuing B.E in the field of I.T from Sinhgad Institute of Technology, Lonavala***.**

Jai Kannan
*Pursuing B.E in field of I.T from Sinhgad Institute of Technology, Lonavala***.**

Deep Utkal Shah
Pursuing B.E in field of I.T from Sinhgad Institute of Technology, Lonavala.