Offensive Decoy Technology for Cloud Data Attacks

[1]Lingaswami, [2]G. Avinash Reddy,

[1]*PG Scholar, Department of Information Technology, TKR College of Engineering and Technology*
Hyderabad, A.P-500 097, India

[2]*Assistant Professor, Department of Information Technology, TKR College of Engineering and Technology*
Hyderabad, A.P-500 097, India

***Abstract*—**Cloud Computing enables multiple users to, share common computing resources, and to access and store their personal and business information. These new paradigms have thrown new data security challenges. The majority of the cloud users are from the internet. The users those who have valid credentials on the cloud are called insiders. In the security perspective, all the remote users are to be treated as attackers. The security systems should ensure that the remote user is not an attacker. If a valid user's credentials are stolen by an attacker, the attacker can enter into the cloud as a valid user. Distinguishing the valid user and the attacker (the user, who is doing identity crime), the protection of the real user's sensitive data on the cloud from the attacker (insider data theft attacker) and securing the fog cloud with decoy information technology are the major challenges in the field of cloud computing. The Decoy Information Technology is used for validating whether data access is authorized; in the eventuality of any abnormal information access detection it confuses the attacker with bogus information.

***Index Terms*—**Enter key words or phrases in alphabetical order, separated by commas**.**

INTRODUCTION

Over the Internet Cloud computing is the computing services delivery sources. The cloud computing has agility, scalability, elasticity and multi-tenancy. It is believed to have been invented by Joseph Carl Robnett Licklider in the 1960s. From the past 40 years, cloud computing with a lot of lines has developed. Most recent evolution is Web 2.0 being the. Any have, the internet offers only bandwidth which was significant decade before, and for the masses cloud computing has been something developed lately. Over the Internet Now a day's Cloud computing is the computing services delivery sources. The Cloud services gives accessing permissions for businesses and also individuals to utilize software and hardware at remote locations that are maintained by third parties. Some of services of cloud contain social networking sites, online file storage, online business applications, and webmail. The cloud computing model is flexible for information access and computer resources from anywhere that connection of network is available. Cloud computing gives a resources pool which was shared, that also includes networks, data storage space, specialized corporate, user applications and computer processing power.

Features:

The features of cloud computing contains resource pooling, broad network access, on-demand self service, measured and service rapid elasticity. On-demand self service is nothing but customers (normally organizations) can seek and computing resources maintain by their own. Broad network gives permission to use services that are offered over the private or public networks. Pooled resources are nothing but users draw from a computing resources pool, normally in data centers which are remote. Services will be in any form large scaled or small scaled; and utilize of a service is measured and customers are gone increase parallel.

Development:

The cloud computing different service models are

1) Software as a Service (SaaS): SaaS model is a application which was pre-made, additional with any software, hardware network and operating system which are required and provided. Requirement is not there for software license purchasing, and the software application will be run by vendors. In backend the software is updated continuously.

2) Platform-as-a-service (PaaS): The vendor provides and maintains the database, operating system and on certain platforms rest of things is in need to run and the user installs or develops his own software and applications.

3) Infrastructure as a Service (IaaS): The IaaS model gives just the network and hardware; the customer develops or installs its operating systems, applications and software by own. In this rather than software purchasing data center space, servers, and equipment of network, the vendor gives these services and bills the user based on the consumed resources amount.

Deployment of cloud services

Cloud services are typically available through a public cloud private cloud, hybrid cloud, or community cloud. Usually, services which are offered by a public cloud over the Internet and are owned and accessed by a cloud provider.

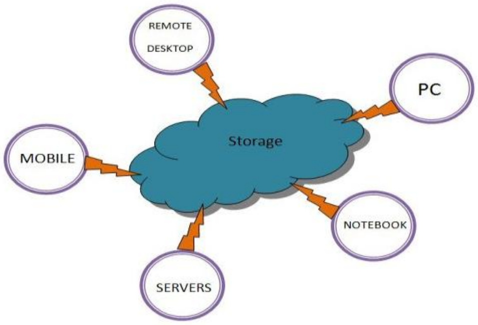
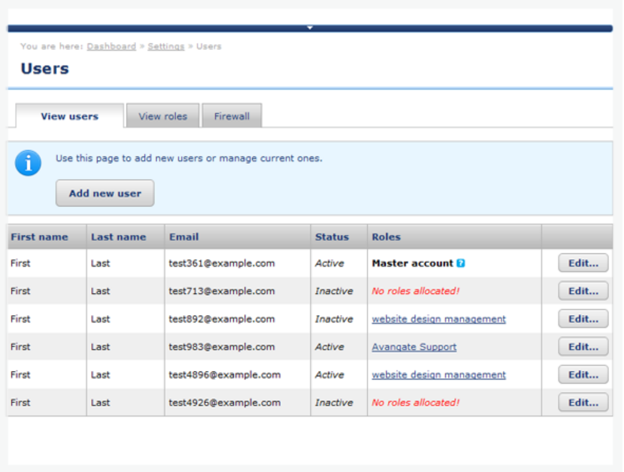


Fig 1: Fog Computing for File Storage

Few of them contain services concerned at the public, such as social networking sites, e-mail services or online photo storage services. Although, enterprises services can also be given in a public cloud.

INSIDER MISUSE DETECTION SYSTEMS OVERVIEW:

The cloud infrastructure in a private cloud is operated single for organization which was specific, and is maintained by a third party or the organization. The service is shared by lot organizations in a community cloud, and access only to those particular groups. The infrastructure may be operated and owned by a cloud service provider or by the organizations.



Users

Use this page to add new users or manage current ones.

First name	Last name	Email	Status	Roles	
First	Last	test361@example.com	Active	Master account	Edit...
First	Last	test713@example.com	Inactive	No roles allocated!	Edit...
First	Last	test892@example.com	Inactive	website design management	Edit...
First	Last	test983@example.com	Active	Avangate Support	Edit...
First	Last	test4896@example.com	Active	website design management	Edit...
First	Last	test4926@example.com	Inactive	No roles allocated!	Edit...

Fig 2: User Access Profiling

File	Directory	Frequency of Access	Operation

Fig 3: User Access Profiling Fields

Top Threats to Cloud Computing V1.0s

This research aims at providing the assistance to organizations to educate on risk management decisions when adopting to cloud strategies. There were seven top threats identified by the research and these threats were evaluated. It discusses the threats in detail with public examples and offers public examples and offers remediation for these threats along with Impact and CSA guidance reference. The threats discussed are:-

1. Nefarious and Abuse use of cloud computing.
2. Interfaces and APIs which are Insecure.
3. Insiders which are Malicious.
4. Technology Issues that was shared.
5. Data leakage or loss.
6. Hacking Account.
7. Unknown Profile which was Risk.

RELATED WORK

Van Dijk et al Approach

In [1] the authors highlights the shift towards thin clients and centralized provision of computing resources in the era of cloud computing. It is also highlighted that due to lack of direct resource control there is data privacy violations, abuse or leakage of sensitive information by service providers. The most powerful tool of cryptography i.e. Fully Homomorphic Encryption (FHE) is one the promising tool to ensure data security. However, the author argues that cryptography alone can't enforce the privacy demanded by common cloud computing services by defining a hierarchy of natural classes of private cloud applications and no cryptographic protocol can implement those classes where data is shared among clients. The author further lays emphasis on the relying on other forms of private enforcement via tamperproof hardware, distributed computing and complex trust eco systems.

Iglesias et al Approach for User Profiling

In [2] an adaptive approach is used for creating behavior profiles and recognizing computer users. It presents an evolving method for updating and evolving user profiles and classifying an observed user. As behavior of the user evolves with time, the behavior is described by fuzzy rules to make them dynamic. It uses the incremental classifier implemented by using trie for automatic clustering, classifier design and classification of the behavior profiles of users. It makes use of Evolving- Profile-Library. As a user behavior changes and evolves, the proposed classifier is able to keep up to date the created profiles using an Evolving systems approach. It is a one pass, non-interactive recursive and can be used in interactive mode. It is computationally very efficient and fast as its structure is simple and interpretable. EVABCD can perform almost as well as other offline classifiers in an online environment in terms of correct classification on validation data, and that it can adapt extremely quickly to new data and can cope with huge amounts of data in a real environment with rapid changes.

Rocha et al Method

In [3] the authors propose that a malicious insider can steal any confidential data of the cloud user in spite of provider taking precaution steps like.

1. Not to allow physical access. 2. Zero tolerance policy for insiders that access the data storage. 3. Logging all accesses to the services and later use for internal audits to find the malicious insider.

It proposes to show four attacks that a malicious insider could do to:-

(i) Compromise passwords.

(ii) Cryptographic keys. (iii) Files and other confidential data. He does it by:- (a) Cleartext passwords in memory snapshots. (b) Obtaining private keys using memory snapshots. (c) Extracting confidential data from the hard disk. (d) Virtual machine relocation. None of these methods ensure to achieve holistic security in the cloud. And the attacker need not be having high technical skills.

Salem et al Methods

The [4] focuses on Masquerade detection to help that means of constructing more dependable and secure systems by their behavior authenticate legitimate users. The author has assumed that each individual user knows his own files are enough to find in a limited and unique fashion to find information. Masqueraders, on the other hand, will likely not know the file system and layout, and would likely search more extensively and broadly in a manner that is different than the victim user being impersonated.

Salem et al Decoy File Management

In the [5] concluded as masquerade attacks pose a grave security problem and detecting masqueraders is very hard. The use of trap-based mechanisms as a means for detecting insider attacks is used in general. In this paper, the author has investigated the use of such trap-based mechanisms for the detection of masquerade attacks. We evaluate the desirable properties of decoys deployed within a user’s file space for detection. The author further investigates the trade-offs between these properties through two user studies, and propose recommendations for effective masquerade detection using decoy documents based on findings from the user studies. The author has presented an experimental evaluation of the different deployment-related properties of decoy documents and a guide to the deployment of decoy documents for effective masquerade detection.

Godoy et al Survey on User Profiling

In the Godoy et al [6] stated the profiling strategies for user profiling. In addition the author discusses the existing approaches and lines of research in the main dimensions of user profiling such as acquisition learning adaptation and evaluation are discussed. The author has discussed in detail the success of personal agents in satisfying user information which intensely relies on the learning approach to acquire user profiles as well as the adaptation strategy to cope with changes in user interests .To better understand user profiling the authors have surveyed the literature regarding the main dimensions involved in the construction of user profiles acquisition learning adaptation and evaluation. Most user-profiling approaches in the agents surveyed had only partially addressed the characteristics that distinguish user profiling of related tasks such as text categorization or supervised learning in general. Future focus on user-profiling approaches for successful information agents not only on the above aspects but also on the assessment of comprehensible semantically enriched user profiles which will take information agents to the next level .The authors have explained the approaches proposed and developed in current personal agents for the main dimensions of user profiling.

Godoy et al Profiling Strategy

The author [7] have helped to address the pressing problems with information overload, the research has developed personal agents to provide assistance to the users in navigating the Web. In addition to provide suggestions, such agents rely on user profiles representing interests and preferences, which makes acquiring and modeling interest categories a critical component in their design. The existing profiling approaches have also been evaluated and they have been found only to be partially tackling the characteristics that distinguish user profiling from related tasks. The author’s technique has generated readable user profiles that have been able to accurately capture the interests, starting from observations of user behavior on the Web. The user-profiling technique which has been demonstrated helps toward the assessment of more comprehensible semantically enhanced user profiles, the application of which can lead to more powerful personal agents, like Personal Searcher, that can accurately identify user interests and adapt their behavior to interest changes. In addition, this technique presents new possibilities regarding users interaction with their profiles as well as collaboration with other agents at a conceptual level.

CLOUD INSIDER ATTACK DETECTION SYSTEM

The Fog Computing Validation requires

System 1: Test Web Application

1. The application should be deployed on a cloud server (VMWare ESX Server). 2. The Application is used to test and to validate the Fog Computing System Detection. The Test Web Applications are the basic

inputs for Fog Computing. All the applications should provide the following options It should store user name, password, confirm password and at least ten secrete questions at the time of account creation It should allow forgot password option by querying the user with randomly selected secret questions.

System 2: Fog Computing System

1. To profile or store the user access behavior 2. It analyzes the present behavior with the past profile. The system has to process The system is an interface to view the anomalous user accesses. It allows the administrators to enforce allow/reject policies for the remote users. It provides logs of anomaly detection system 1. User Access Behavior Profiling 2. Decoy File System Maintenance 3. Anomaly Detection 4. Challenge Requests.

User Access Behavior Profiling

The module is concerned about storing the user's request to files on the web application. The module records how many files read and how often. The operations include create, read, write, delete Fig. 3.

Decoy File System Maintenance

For each newly created folder or a file, corresponding decoy file will be maintained. The directory and file structure are same for both the decoy file system and the original file system. The information contained in the decoy file is not original.

Anomaly Detection

The current logged in user access behavior is compared with the past behavior of the user. If the user behavior is exceeding the threshold value or a limit, then the remote user is suspected to be anomaly. If the current user behavior is as the past behavior, the user is allowed to operate on the original data.

Challenge Requests

If the current user's behavior seems anomalous, then the user is asked for randomly selected secret questions. If the user fails to provide correct answers for a certain limits or threshold, the user is provided with decoy files. If the user provided correct answers for a limit, the user is treated as normal user. sub subsection System 3: Web Server It provides an environment to deploy the application. On every access, it stores or log the following details Client IP, Uid, PID, Time Stamp, Request, Response Code, Response Length, Referer and User-Agent.

Example:

```
192.168.1.1 - - [14/Aug/2012:11:34:57 -0700] ”POST /cwt/installation/index.php HTTP/1.1” 200 214 ”http://www.abc.com/index.php” ”Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.1 (KHTML, like Gecko) Chrome/21.0.1180.75 Safari/537.1”
```

System 4: Internet Users

The users of the cloud can be from anywhere of the internet.

System 5: Administration System (Web Sphere / Web Interface)

The system is an interface to view the anomalous user accesses. It allows the administrators to enforce allow/reject policies for the remote users. It provides logs of anomaly detection system. The system is an interface to view the anomalous user accesses. It allows the administrators to enforce allow/reject policies for the remote users. It provides logs of anomaly detection system.

CONCLUSION

Monitoring the activity of the cloud storage user in Infrastructure as a service (IaaS) cloud environments is an important work. The authors proposed several techniques for identifying the misuser or attacker in the cloud. But there are no efficient profiling strategies for cloud storage area protection and there are no clear distinguishing strategies for identifying the attacker's activity. Hence, proposing an efficient strategy for quickly adopting the user's behavior.

REFERENCES

[1] M. Van Dijk and A. Juels, “On the impossibility of cryptography alone for privacy-preserving cloud computing,” in Proceedings of the 5th USENIX conference on Hot topics in security, ser. HotSec'10. ”Berkeley, CA, USA”: ”USENIX Association”, 2010, pp. 1–8.

[2] J. A. Iglesias, P. Angelov, A. Ledezma, and A. Sanchis, “Creating evolving user behavior profiles automatically,” IEEE Trans. on Knowl. and Data Eng., vol. 24, no. 5, pp. 854–867, May 2012.

[3] F. Rocha and M. Correia, “Lucy in the sky without diamonds: Stealing confidential data in the cloud,” in Proceedings of the 2011 IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops, ser. DSNW '11. Washington, DC, USA: IEEE Computer Society, 2011, pp. 129–134.

[4] M. B. Salem and S. J. Stolfo, “Modeling user search behavior for masquerade detection,” in Proceedings of the 14th international conference on Recent Advances in Intrusion Detection, ser. RAID'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 181–200.

[5] S. et al, “Decoy document deployment for effective masquerade attack detection,” in Proceedings of the 8th international conference on Detection of intrusions and malware, and vulnerability assessment, ser. DIMVA'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 35–54.

[6] D. Godoy and A. Amandi, “User profiling in personal information agents: a survey,” Knowl. Eng. Rev., vol. 20, no. 4, pp. 329–361, Dec. 2005.

[7] D. Godoy, “User profiling for web page filtering,” IEEE Internet Computing, vol. 9, no. 4, pp. 56–64, Jul. 2005.

[8] Cloud Security Alliance, “Top Threat to Cloud Computing V1.0,” March 2010. [Online]. Available: https://cloudsecurityalliance.org/topt hreats/csathreats.v1.0.pdf

[9] P. Allen, “Obama's Twitter password revealed after french hacker arrested for breaking into U.S. president's account,” March 2010. [Online].Available: http://www.dailymail.co.uk

/news/article-1260488/Barack- Obamas-Twitter-password-revealed-French-hacker-arrested.html

[10] 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.[Online].Available: https://mice.cs. columbia.edu/getTechreport.php?techreportID=1468*