Survey on Defense against Insider Misuse Attacks in the Cloud

J Venkata Subbarayudu [α] & Shaik Jakeer Hussain [σ]

Abstract - **Cloud computing provides highly scalable services for the purpose of online usage as daily premises. A key thing in cloud services is that users keeps processing in the unknown fashion where they are not aware of machines working on which are not operating by them. After all with the new technology they are adopted to now users' scares of their data which was uploaded in cloud. This appears a significant barrier due to adoptability nature of cloud network. For exploring this problem or threat we prefers a novel perfectly decentralized data computational framework for the records of accessing details of the users' information in the cloud. Clearly, we prefers or proposes an object-centered schema which makes active of accessing together with users' data and policies. We makes benefit the JAR programmable features to both develop a dynamic and random object, and to provide accessing to users' information will contains the authenticating formalities and automated accessing local to the JARs. For the improvement of user's maintenance, and also providing distributed auditing mechanisms. In additional we gave researches information which are practically done that explains the efficiency and effectiveness of this way of approaching.**

I. Introduction

Cloud computing is the network that which provides its services among online. There are no particular restrictions in the cloud computing each and every normal user can utilizes this thing at the same time big organizations are capable to use software and hardware that are under by third parties from different localities. Cloud applications in reality are so many they are used everywhere in social networking sites, search engines etc. This is cause of flexible nature of cloud computing people can get through connected anywhere anytime with simple internet connection. Cloud computing gives restriction less of resources like data base where the information stores, networks, computer processing power, and commercial organizations and customer apps.

Cloud computing explores a new path for the users for the random development in the technology, by making dynamically scalable and virtualized resources as a service through online applications. A recent Microsoft survey found that almost more than half of the people are placing or using the cloud for their transmissions but they are afraid of security of their data which was placed. At last, users are not aware of machines working on which are not operating by them.

Now users' scares of their data which was uploaded in cloud. The data which was present on clouds consist of different types of categories such as financial, business and may be personal information. This creates a significant barrier due to adoptability nature of cloud network.

a) Features

The features of cloud computing contains on-demand self service, huge network access, resource stream, flexibility and efficient service. On-demand self service is the feature that user is capable of maintaining their own computing resources. Huge network access gives services over the online or organization individual networks. Pooled resources means users draw from a pool of computing resources, from remote data centers. Services will gone be provided to the user based upon the payments by the particular user.

b) Service Methods

The service methods are:

1) Software as a Service (SaaS): It is a system application that comes along with system itself. In PaaS, an operating system, hardware, and network are provided, and if any other external application has to be install it will be done by user itself.
2) Infrastructure as a Service (IaaS): The IaaS model is used for organization equipment to help operations; those operations are nothing but storage, hardware, servers and networking components. The service provider contains itself equipment and takes care of maintenance. The user pays for it as per usage basis.

c) Deployment of cloud services

Cloud services are available by different ways a cloud for private organizations, group cloud, general cloud or hybrid cloud. Public clouds are nothing but the social services through online and are operated by a cloud provider. Those apps targeted at the general, like online photo storage in search engine services, electronic mail, and social net working sites. Any have, services for enterprises have chances offered in a general/public cloud. In a cloud of private organizations, the cloud architecture is maintained solely for a particular organization, and is observed or maintained by the organization itself or by a third party. In a community/group cloud, the service is shared by different organizations and gives access to those

Authors α σ : M. Tech, CSE Dept, ASRA Hyderabad
E-mails : venkat07509@gmail.com, jakeerhussiansk@gmail.com

particular groups only. The infrastructure /architecture will be maintained under organizations or by a cloud service provider.

II. Insider Misuse Detection Systems Overview

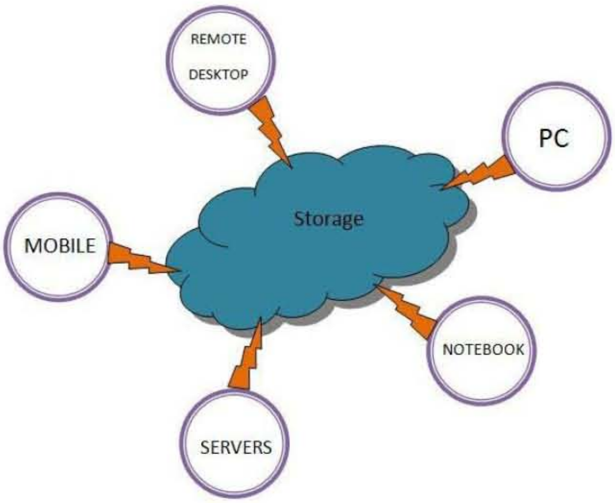
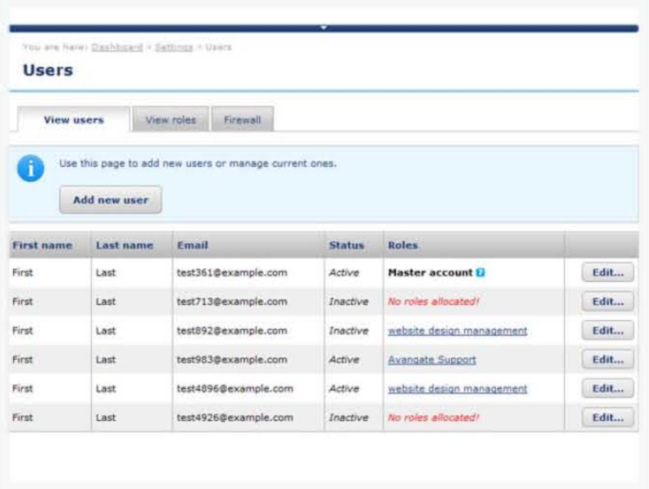


Figure 1 : Fog Computing for File Storage

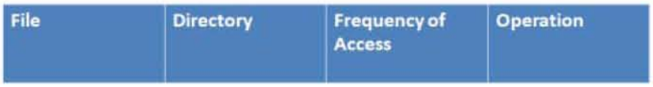

You are here: Dashboard > Settings > Users

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...

Figure 2 : User Access Profiling



File	Directory	Frequency of Access	Operation

Figure 3 : User Access Profiling Fields

III. Survey on Insider Misuse Attack Detection

a) Top Threats to Cloud Computing V1.0

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. Abuse and Nefarious use of cloud computing.
2. Insecure Interfaces and APIs.
3. Malicious Insiders.
4. Shared Technology Issues.
5. Data loss or leakage.
6. Account or service Hijacking.
7. Unknown Risk Profile.

b) Van Dijk et al Approach

In 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 viz tamperproof hardware, distributed computing and complex trust eco systems.

c) Iglesias et al Approach for User Profiling

In an adaptive approach 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.

d) Rocha et al Method

In the authors propose that a malicious insider can steal any confidential data of the cloud user inspite 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) Clear text 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.

e) Salem et al Methods

The focuses on Masquerade detection to serve as a means of building more secure and dependable systems that authenticate legitimate users by their behavior. The author has assumed that each individual user knows his own file system well enough to search 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. A categorization of Windows applications and user commands that are used to abstract sequences of user actions and identify actions linked to search activities is devised. The use of search behavior profiling for masquerade attack detection permits limiting the range and scope of the profiles we compute about a user, thus limiting potentially large sources of error in predicting User search behavior modeling produces better accuracy. With the use of the RUU dataset, the best results achieved and reported in literature to date: 100% masquerade detection rate with only 1.1% of false positives. The limited set of features used for search behavior modeling also results in large performance gains over the same modeling techniques that use larger sets of features. The author has proposed an approach to profile a user's behavior based on taxonomy of Windows applications.

f) Salem et al Decoy File Management

In the 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.

g) Godoy et al Survey on User Profiling

In the Godoy et al stated the profiling strategies for user profiling. Personal information agents have emerged in the last decade to help users to cope with the increasing amount of information available on the Internet. These agents are intelligent assistants that perform several information- related tasks such as finding, filtering and monitoring relevant information on behalf of users or communities of users. In this paper the author presents a summary of the state-of-the-art in user profiling in the context of intelligent information agents. 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.

h) Godoy et al Profiling Strategy

The author 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 user's interaction with their profiles as well as collaboration with other agents at a conceptual level.

IV. Cloud Insider Attack Detection Proposal

The Fog Computing Validation requires

a) 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 question.

b) 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.

c) 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.

d) 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.

e) 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.

f) 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, Referrer and User-Agent.

Example :

```
192.168.1.1 - - [14/Aug/2012:11:34:57 -0700] "POST/cw
t/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) Chro
me/21.0.1180.75 Safari/537.1"
```

g) System 4: Internet Users

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

h) System 5: Administration System (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 en- force allow/reject policies for the remote users. It provides logs of anomaly detection system

V. Conclusion

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

References Références Referencias

1. P. Ammann and S. Jajodia, "Distributed Timestamp Generation in Planar Lattice Networks," ACM Trans. Computer Systems, vol. 11, pp. 205-225, Aug. 1993.
2. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. ACM Conf. Computer and Comm. Security, pp. 598-609, 2007.
3. E. Barka and A. Lakas, "Integrating Usage Control with SIP-Based Communications," J. Computer Systems, Networks, and Comm., vol. 2008, pp. 1-8, 2008.

4. D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology, pp. 213-229, 2001.
5. R. Bose and J. Frew, "Lineage Retrieval for Scientific Data Processing: A Survey," ACM Computing Surveys, vol. 37, pp. 1-28, Mar. 2005.
6. P. Buneman, A. Chapman, and J. Cheney, "Provenance Management in Curated Databases," Proc. ACM SIGMOD Int'l Conf. Management of Data (SIGMOD '06), pp. 539-550, 2006.
7. B. Chun and A.C. Bavier, "Decentralized Trust Management and Accountability in Federated Systems," Proc. Ann. Hawaii Int'l Conf. System Sciences (HICSS), 2004.
8. OASIS Security Services Technical Committee, "Security Assertion Markup Language (saml) 2.0," http://www.oasis-open.org/committees/tchome.php ?wg abbrev=security, 2012.
9. R. Corin, S. Etalle, J.I. den Hartog, G. Lenzini, and I. Staicu, "A Logic for Auditing Accountability in Decentralized Systems," Proc. IFIP TC1 WG1.7 Workshop Formal Aspects in Security and Trust, pp. 187-201, 2005.
10. B. Crispo and G. Ruffo, "Reasoning about Accountability within Delegation," Proc. Third Int'l Conf. Information and Comm. Security (ICICS), pp. 251-260, 2001.
11. Y. Chen et al., "Oblivious Hashing: A Stealthy Software Integrity Verification Primitive," Proc. Int'l Workshop Information Hiding, F. Petitcolas, ed., pp. 400-414, 2003.
12. S. Etalle and W.H. Winsborough, "A Posteriori Compliance Control," SACMAT '07: Proc. 12th ACM Symp. Access Control Models and Technologies, pp. 11-20, 2007.
13. X. Feng, Z. Ni, Z. Shao, and Y. Guo, "An Open Framework for Foundational Proof-Carrying Code," Proc. ACM SIGPLAN Int'l Workshop Types in Languages Design and Implementation, pp. 67-78, 2007.
14. Flickr, http://www.flickr.com/, 2012.

This page is intentionally left blank