SURVEY ON INSIDER DATA THEFT MISUSE ATTACKS IN THE CLOUD

G. Dileep Kumar[1], Kolla Morarjee[2]

[1]M.Tech scholar, Department of Computer Science and Engineering, CMR Institute of Technology,
Medchal, 501401, Hyderabad, Andhra Pradesh, India
dileepkumar.gattu569@gmail.com

[2]Assistant Professor, Department of Computer Science and Engineering, CMR Institute of Technology,
Medchal, 501401, Hyderabad, Andhra Pradesh, India
morarjeek@gmail.com

Abstract

Cloud Computing enables multiple users to, share common resources, and to store their personal and business information and access them. The major of the cloud users are from the internet. The users those who have valid authority on the cloud are called insiders. In all the remote users are to be treated as attackers in the security perspective. If the remote user is not an attacker then that should be checked by the security systems. If a valid user's access details are stolen by an attacker, then attacker can enter and access the cloud as a valid user. Distinguishing the valid user and the attacker, the protection of the real user's sensitive data on the cloud from the 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.

Keywords: Fog computing, decoy information, decoy technology, data access, and malicious insider.

1. Introduction

Cloud computing is the delivery of computing services over the Internet. The cloud computing has agility, scalability, elasticity and multi-tenancy. Since the sixties, cloud computing has developed. The internet only started to offer meaningful bandwidth in the nineties. Now a days, Cloud computing is the delivery of computing services on the Internet. The Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. The cloud services include social networking sites, online file storage, online business applications and webmail. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. The cloud computing provides an shared pool of resources, including networks, data storage space, computer processing power, user applications and specialized corporate.

The characteristics of cloud computing include on-demand broad network access, self service, measured service, resource pooling and rapid elasticity. Self service means that customers can manage and request their own resources. In the Internet or private networks the services to be offered are known as Broad network access. Pooled resources, the customers draw from a pool of computing resources, usually in remote data centers. The services can scale larger or smaller, and customers are billed accordingly to the use of a service is measured.

The cloud computing service models are discussed below as:

1) Software as a Service (SaaS): In a Software as a Service model, a pre-made application, along with any operating system, required software, network and hardware are provided. There is no requirement of purchasing a software license, and the vendors run the software application for you.

2) Platform-as-a-service (PaaS): The vendor provides and manages the database, operating system, and everything else needed to run on certain platforms and the customer installs or develops his own software and applications.

3) Infrastructure as a Service (IaaS): The customer installs or develops its own operating systems, software and applications. In this rather than purchasing data center space, software, servers, and network equipment, for these services the vendor provides and bills to clients for the amount of resources consumed.

Cloud services are typically made available via a community cloud, private cloud, hybrid cloud or public cloud. Generally speaking, services providing by a public cloud will be offered over the internet and are operated and owned by a cloud service provider. Some examples include services at the general public, such as e-mail services, online photo storage services, or social networking sites in the web. In public cloud, services for enterprises can also be offered. However, cloud infrastructure is operated solely for a specific organization or a third party. In a cloud community, several organizations share the service and made available only to those groups. The cloud service provider may be owned and operated the infrastructure.

INSIDER MISUSE DETECTION SYSTEMS

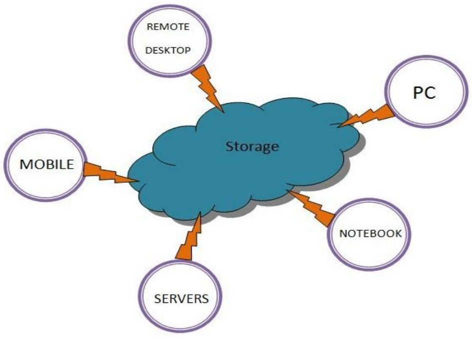

Fig. 1 Fog Computing for File Storage

2. Literature survey

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

Van Dijk et al in [1] proposed Cloud-Application Class Hierarchy that shift towards thin clients and centralized provision of computing resources in the era of cloud computing. It is also strongly illuminated 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. The 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 disadvantage is Abuse and Nefarious use of cloud computing

Iglesias p et al in [2] proposed 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 to develop with time, the method is described by fuzzy rules to make them dynamic. It makes use of Evolving- Profile-Library. As a user behavior changes and evolves the classifier is able to keep up to date the created profiles using an Evolving systems approach. It is a one pass, non-interative recursive and can be used in interactive mode. It is operating very efficient and fast as its structure is interpretable and simple. 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. The disadvantage is Insecure Interfaces and APIs.

Rocha F et al in [3] proposed 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 and (iii) Files and other confidential data like, cleartext passwords in memory snapshots, obtaining private keys using memory snapshots, extracting confidential data from the hard disk and Virtual machine relocation. The disadvantage is Malicious Insiders

Salem B et al in [5] proposed an masquerade for the detection trap-based mechanisms and 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. The use of such trap-based mechanisms for the detection of masquerade attacks. The desirable properties of decoys deployed within a user's file space for detection. The trade-offs between these properties through two user studies, and proposes recommendations for effective masquerade detection using decoy documents based on findings from the user studies. The different deployment-related properties of decoy documents and a guide to the deployment of decoy documents for effective masquerade detection. The disadvantage is Shared Technology Issues and Data loss or leakage.

Godoy et al in [8] 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. Here, this technique 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 on 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 disadvantage is Account or service Hijacking

Salvatore J.S et al [6] proposed an approach for securing data in the cloud using fog computing. In this we monitor data access in the cloud and detect illegal data access patterns. The Fog computing uses decoy information technology to launch disinformation attacks against malicious insiders and preventing them from distinct real sensitive customer data from fake worthless data. In this, we can decrease the value of stolen information by decreasing the damage of stolen data. The secure cloud services can be implemented given two additional security features: 1) User Behavior Profiling User profiling is a well known technique that can be applied here to know how much a user accesses their information in the Cloud. 2) Decoys are confuse an adversary into believing they have ex-filtrated useful information and validating whether data access is authorized or unauthorized access is detected then confusing the attacker with bogus information. This technology may be used with User behavior profiling technology to secure a user's information in the Cloud.

3. Conclusions

This paper presents a survey on various cloud computing risks that were proposed by earlier researches for the better development in the field of Cloud computing. Various algorithms and methods discussed above will help in developing efficient and effective for finding the fog misuse or attacker for cloud computing. In the future scope, we will be presenting a comparative study of various algorithms for cloud computing.

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] M. B. Salem and S. J. Stolfo , "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] 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.

[7] A salya and Ravi M, "survey on defense against insider misuse attacks in the cloud", in Proceedings of the international journals of advanced computing , vol.5, no.1, 2013.

[8] 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.

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

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

[11] P. Allen, "Obama's Twitter password revealed after french hacker arrested for breaking into U.S. president's account," March 2010.

[12] 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