

Instigate Security in Cloud computing using Profile of User Behavior and Decoy Technology

K.Shanthi

PhD Research Scholar

Prist University, Thanjavur, India

Abstract— Cloud computing refers a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing is a place for the users to host their web services such as web hosting and cloud storage. This has attracted the hackers to steal the business data, such as daily sales, profit reports, financial reports etc. The types of cloud attacks are malware injection attack, wrapping attack, SQL injection, authentication attack and Denial of Service. The “hot button” issues surrounding cloud computing relate to storing and securing data, and monitoring the use of the cloud by the service providers. These issues are generally attributed to slowing the deployment of cloud services. These challenges can be addressed, for example, by storing the information internal to the organization, but allowing it to be used in the cloud. For this to occur, though, the security mechanisms between organization and the cloud need to be robust. There are numerous algorithms implemented to secure data. User behavior profiling and decoy technology provide a better way to secure data on a server, which is more efficient and secure. There are many algorithms on user behavior profiling and decoy technology but no one can find the problem is that efficiently delivering the decoy file in such a way the intruder not able to recognize the difference between the genuine and decoy file, once the anonymous behavior of the user identified. Proposed a system in which we are going to use the two techniques together i.e user behavior profiling and decoy technology.

Key words: Security, Cloud Computing, Decoy Technology, User Behavior Profiling, Denial of Service

I. INTRODUCTION

Cloud computing consists of a shared pool of resources shared among users per subscription basis. The way computer-stored information and personal data can cause new data security challenges. In today's world scenario every organization using cloud computing to protect their data and to use the services like Iaas, Paas, Saas. Encryption mechanism, that we use today in order to protect the data over the cloud are not fair enough to stop the unauthorized access to genuine user data.

Thus, we proposed a system in which we are going to use the two techniques together i.e. user behavior profiling and decoy technology; a different approach for securing data in cloud using offensive decoy technology. In this, when the unauthorized person try to access the data of the real user, the system generates a fake documents in such a way that the unauthorized person was not able to identify that the data is fake or real.

A. 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' behaviour 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.

B. Decoy Technology

Decoy data, such as decoy documents, honey pots and other bogus information can be generated on demand and used for detecting unauthorized access to information and to poison the thief's ex-filtrated information. Serving decoys will confuse an attacker into believing they have ex-filtrated useful information, when they have not.

Whenever abnormal and unauthorized access to a cloud service is noticed, decoy information may be returned by the Cloud and delivered in such a way that it appear completely normal and legitimate. The legitimate 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 incorrectly 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 attacker, thus securing the user's true data from can be implemented by given two additional security features:

- 1) Validating whether data access is authorized when abnormal information access is detected
- 2) Confusing the attacker with bogus information that is by providing decoy documents.

II. EXISTING SYSTEM

There are many algorithms on user behavior profiling and decoy technology but no one addresses the problem of efficiently delivering the decoy file in such a way the intruder not able to recognize the difference between the genuine and decoy file, once the anonymous behavior of the user identified. The existing system was not worked on anonymous behavior. The data stored on cloud need security for stored data. The way computer-stored information and personal data can cause new data security challenges. Encryption mechanism, that we use today's in order to protect the data over the cloud is not fair enough to stop the

unauthorized access to genuine user data. As we know that previously we have traditional database system deployed in local network access locally only. As the size of the Internet increases day by day and because of the new computing technology like distributed computing technology, by which anybody can access the database from anywhere around the world, arises the problem of security. Existing encryption-based data protection mechanism fails most of the time in securing data from the intruders. Encryption mechanism doesn't verify the identity of the intruders, instead of that, they focus only on the key provided by the users at the time of accessing the available resources which may or may not provide by the authenticated user.

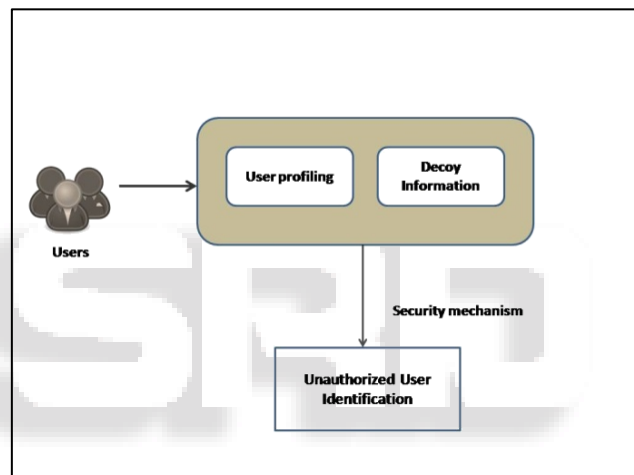
On cloud encryption-based data protection mechanism fails most of the time in securing data from the intruder's. On a cloud, we see if intruder gain access to our cloud anyhow then our information got compromised in many unknowingly ways In order to reduce the amount of damage done by the intruder once the key is compromised reduce by employing the technique of User behavior profiling and offensive decoy technology.

III. REVIEW OF LITERATURE

- 1) This paper presents a high-level classification of current research in cloud computing security. Unlike past work, this classification is organized around attack strategies and corresponding defences. Specifically, we outline several threat models for cloud computing systems, discuss specific attack mechanisms, and classify proposed defences by how they address these models and counter these mechanisms [3].
- 2) Proposed 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. We investigate the trade-offs between these properties through two user studies and propose recommendations for effective masquerade detection using decoy documents based on findings from our user studies[2].
- 3) Paper identifies the possible security attacks on clouds including Wrapping attacks, Malware-Injection attacks, Flooding attacks, Browser attacks, and also Accountability checking problems. We identify the root causes of these attacks and propose specific solutions[6].
- 4) The cloud hook formation provides a useful analogy for cloud computing, in which the acutest obstacles with outsourced services (i.e., the cloud hook) are security and privacy issues. This paper identifies key issues, which are believed to have long-term significance in cloud computing security and privacy, based on documented problems and exhibited weaknesses[7].
- 5) The subsisting methods of protecting data on the cloud have failed in preventing data theft attacks. An altered approach is carried out for securing the data, in addition to the previous standard encryption mechanisms. The technologies are – 1) User Behavior Profiling and 2) Decoy Technology. The users using the Cloud are monitored and their access patterns are recorded. Every User has a distinct profile which is monitored and updated. When an abnormal activity such as

- 6) Present two provably-secure PDP schemes that are more efficient than previous solutions, even when compared with schemes that achieve weaker guarantees. In particular, the overhead at the server is low (or even constant), as opposed to linear in the size of the data.[13].
- 7) In the network, malicious nodes are responsible to trigger various types of active and passive attacks which reduce network performance in terms of various parameters. In this work, the technique will be proposed for the detection and isolation of malicious nodes from the network. the malicious nodes are responsible to trigger virtual side channel attack in the network.[14].

IV. PROPOSED SYSTEM OVERVIEW



Proposed a completely new technique in order secure the data over the cloud using the user behavior profiling and a new offensive decoy technology. We monitored the data access over the cloud and try to detect the abnormal access pattern over the cloud. In this system whenever an intruder tries to access the data of the genuine user, we automatically generate a decoy file with the same name and scrambling content file in such a way it looks genuine as the targeted file and provides the same to the intruder. User Profiling technique applied hear to model how, when, and how much amount of information access by the user over the cloud. Such normal behavior of the user is continuously monitored to determine whether or not abnormal access to a user's information is occurring. Depicted behavior-based security mostly used by cops in fraud detection. Decoy technology is used in way by validating; whether the data access is authorized or unauthorized when abnormal behavior is detected.

It is identified thought the question which is entered by the real user at that time of filling the form. If the answer of the question is wrong it means the user is not the real user and the system provide the fake document else original document will be provided to the real user by the system.

Confusing the unauthorized user with a bogus amount of decoy information, which is provided by the decoy

document, is generated once the behavior of the user is being identified as anonymous using user behavior profiling technology. The generated file should be as such that the content of the original file and decoy file are completely different and not easy to identifiable.

User: Login, Register, Search file, Download file

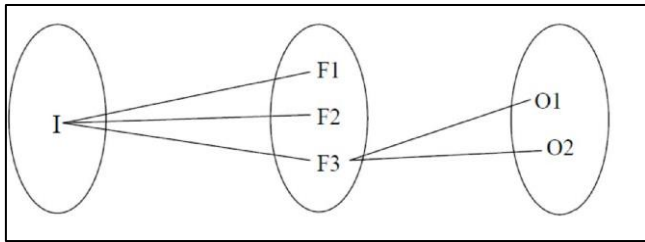
Intruder: Behave wrong by entering the wrong password, Get decoy file

Admin: View Users, View hackers downloaded file

– Advantages:

- 1) Anonymous behavior will find and he can get decoy file.
- 2) It confirms first whether a requested user is authenticated or not.

A. Mathematical Model:



Let, S be the System Such that,

A= {I, O, F, success, failure}

Where,

I= Login details

O= Decoy file

F =Detecting user behavior and Download decoy file

– Input:

I=Enter invalid login details.

– Function:

F1=Check user login details

F2= find Anonymous activity

F3= if user behavior is illegal to download decoy file

– Output:

O1=Success Case (the user is behaving normally it will get original file and if anonymous will get decoy file)

O2=Failure Case

- 1) A huge database can lead to more time consuming to get the information.
- 2) Hardware failure.
- 3) Software failure

V. CONCLUSION

With the increase of data, theft attacks the security of users private data over the cloud is becoming a serious issue for cloud service providers. For which, Fog Computing is a technique which helps in predicting and monitoring the behavior of the user and providing security to the user's data. The system was originally developed using encryption algorithm but we have also implemented it with the user behavior profiling algorithm along with dynamically generated decoy file system concept. The proposed system scramble the data of the file that is hacker will not recognize a difference between the original file and scrambled file.

REFERENCES

- [1] Prevention Of Malicious Insider In The Cloud Using Decoy Documents by S. Muqtyar Ahmed, P. Namratha, C. Nagesh
- [2] Cloud Security Alliance, Top Threat to Cloud Computing V1.0, March 2010.
- [3] Cloud Security: Attacks and Current Defenses Gehana Booth, Andrew Soknacki, and Anil Somayaji.
- [4] Overview of Attacks on Cloud Computing by Ajay Singh,Dr. Maneesh Shrivastava
- [5] D.Jamil and H. Zaki, Security Issues in Cloud Computing and Countermeasures, International Journal of Engineering Science and Technology, Vol. 3 No. 4, pp. 2672-2676, April 2011.
- [6] K. Zunnurhain and S. Vrbsky, Security Attacks and Solutions in Clouds, 2nd IEEE International Conference on Cloud Computing Technology and Science, Indianapolis, December 2010.
- [7] W. A. Jansen, Cloud Hooks: Security and Privacy Issues in Cloud Computing, 44th Hawaii International Conference on System Sciences, pp. 110, Koloa, Hawaii, January 2011.
- [8] F. Bonomi, Connected vehicles, the internet of things, and fog computing,” in The Eighth ACM International Workshop on Vehicular Inter-Networking(VANET), Las Vegas, USA, 2011”.
- [9] Fog Computing: Mitigating Insider Data Theft Attacks in The Cloud.
- [10] 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, HotSec10. Berkeley, CA, USA: USENIX Association, 2010, pp. 18.
- [11] 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. RAID11. Berlin, Heidelberg: Springer Verlag, 2011, pp. 181200.
- [12] Setal, 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. DIMVA11. Berlin, Heidelberg: Springer-Verlag, 2011
- [13] Giuseppe Ateniese, Randal Burns† Reza Curtmola, Joseph Herring† Lea Kissner, Zachary Peterson† Dawn Song, Provable Data Possession at Untrusted Stores
- [14] Komal Jeet Kaur , Technique for Isolation of Malicious Nodes from the Cloud Computing Architecture International Journal Of Engineering And Computer Science ISSN:2319-7242Volume 6 Issue 7 July 2017, Page No. 22079-2208
- [15] Tejas R. Kulkarni,Varad Waghmare, Dilip Chaudhary, Parth Kulkarni, Security Implementation in cloud computing using User Behavior Profiling and Decoy Technology ,World journal of Technology, Engineering and Research.