SECURITY IMPLEMENTATION IN CLOUD COMPUTING USING USER BEHAVIOR PROFILING ALGORITHM AND DECOY TECHNOLOGY

G.Blessy
CSE - Department
Adhiyamaan college of engineering - Hosur
S.Heena
CSE - Department
Adhiyamaan college of engineering - Hosur
N.Ishwarya
CSE - Department
Adhiyamaan college of engineering - Hosur

Abstract: Cloud is the cluster of geographically connected network bearing information. Cloud Computing make feasible for multiple users to, share common computing resources, and to access and store their personal and business information. In cloud computing we stored data on server side as well on client side. Application like Drop box provides service in such a way that data on server and on client machine are synchronous. So implementing security become very necessary on client side. Traditional algorithm failed once key is compromised. User behavior profiling and decoy technology provide an alternate way to secure data on server which is more efficient and secure. There are many algorithms on user behavior profiling and decoy technology but no one address 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. We proposed a system in which we going to use the two technology together i.e. user behavior profiling and decoy technology and also check the connection

port also. We also proposed the mechanism by which we generate the decoy file in such a way it matches the content of the genuine file up to the accuracy of 98 percent.

II. 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 going to use the two techniques together i.e. user behavior profiling and decoy technology. Into 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. 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.

Cloud Services are subscription based services. Cloud computing consists of shared pool of resources shared among users per subscription basis. The way computer stored information and personnel 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 un-authorized access of 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 database from anywhere around the world, arises the problem of security], synchronization etc. By registering into the cloud user ready to excess the resources anywhere around the world, at any point of time they needed for personnel/organizational work.

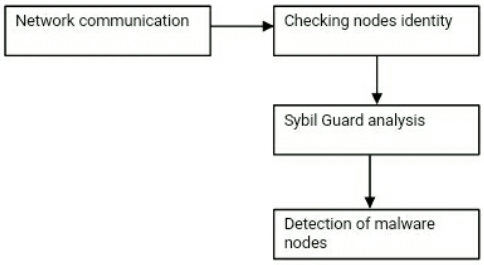
But above comfortless involve the risk of data compromise and security. To overcome the issue of security and privacy we introduce the new

technique called as Fog Computing. Once user registered with our services, users automatically start getting our services without the need of change of any short of hardware either at client end or at server end.

Malicious Insider

Insider attacks can be performed by malicious employees at the providers or user's site. Malicious insider can steal the confidential data of cloud users. This threat can break the trust of cloud users on provider. A malicious insider can easily obtain passwords, cryptographic keys and files. These attacks may involve various types of fraud, damage or theft of information and misuse of IT resources. The threat of malicious attacks has increased due to lack of transparency in cloud providers processes and procedures. It means that a provider may not reveal how employees are granted access and how this access is monitored or how reports as well as policy compliances are analyzed. Additionally, users have little visibility about the hiring practices of their provider that could open the door for an adversary, hackers or other cloud intruders to steal confidential information or to take control over the cloud. The level of access granted could enable attackers to collect confidential data or to gain complete control over the cloud services with little or no risk of detection. Malicious insider attacks can damage the financial value as well as brand reputation of an organization.

Sybil Guard:



SYBIL attacks refer to individual malicious users creating multiple fake identities (called *Sybil identities* or *Sybil nodes*) in *open-access* distributed systems (such as peer-to-peer systems). These open-access systems aim to provide service to any user who wants to use the service (instead of, for example, only to a predetermined group of 10 users). Sybil attacks have already been observed in the real world] in the Maze peer-to-peer system. Researchers have also demonstrated that it is surprisingly easy to launch Sybil attacks in the widely used mule system. When a malicious user's Sybil nodes comprise a large fraction of the nodes in the

system, that one user is able to "outvote" the honest users in a wide variety of collaborative tasks.Examples of such collaborative tasks range from Byzantine consensus and voting schemes for e-mail spam to implicit collaboration in redundant routing and data replication in distributed hash tables (DHTs). The exact form of such collaboration and the exact fraction of Sybil nodes these collaborative tasks can tolerate may differ from case to case. However, a generic requirement for thwarting such attacks is that the number of Sybil nodes (compared to the number of honest users) needs to be properly bounded. Sybil attacks can be thwarted by a trusted central authority if the authority can tie identities to actual human beings, but implementing such a capability can be difficult or impossible, especially given the privacy concern of the users. Another approach is for the central authority to impose a monetary charge on each identity, which is, however, undesirable in many applications. Without these trusted central authorities, defending against Sybil attacks is much harder. Among the small number of approaches, the simplest one perhaps is to bind identities to IP addresses or IP prefixes. Another approach is to require every identity to solve puzzles that require human effort, such as CAPTCHAs. Both approaches can provide only limited protection—the adversary can readily steal IP addresses with different prefixes in today's Internet while CAPTCHAs can be reposted on an adversary's Web site to be solved by users seeking access to that site. In fact, Douceur's initial paper on Sybil attacks already proved a negative result showing that Sybil attacks cannot be prevented unless special assumptions are made.

III. LITERATURE SURVEY

1. Prevention of Malicious Insider in the Cloud Using Decoy Documents

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network. Cloud computing entrusts remote services with a user's data, software and computation. 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. The data protection mechanisms such as encryption have failed in preventing data theft attacks, especially those illegal actions by a malicious insider2 to the cloud. Much research in cloud computing security has focused on ways of preventing malicious insider and illegitimate access to data. A different approach to secure the cloud using decoy information technology, which we have, come to call Fog computing3. Decoys4 are used to launch disinformation attacks against malicious insiders, preventing them from distinguishing the real sensitive customer data from fake worthless data. Alert message is issued to authenticated user.

2. Cloud Security: Attacks and Current Defenses

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 defenses. Specifically, we outline several threat models for cloud computing systems, discuss specific attack mechanisms, and classify proposed defenses by how they address these models and counter these mechanisms. This examination highlights that, while there has been considerable research to date, there are still major threats to cloud computing systems, such as potential infrastructure compromise, that need to be better addressed.

3. Overview of Attacks on Cloud Computing

Cloud Computing is a new environment in computer oriented services. This system have some similarities of distributed system, according to this similarities cloud computing also uses the features of networking. Therefore the security is the biggest problem of this system, because the services of cloud computing is based on the sharing. In this paper we discussed the different types of attack in cloud computing services and cloud wars also

4. Security Issues in Cloud Computing and Countermeasures

Cloud computing represents a relatively new computing model in the evolution of on-demand information technology services and products, that is built on decades of research in virtualization, distributed

computing, utility computing, and more recently networking, web and software services. It implies a service oriented architecture, reduced information technology overhead for the end-user, great flexibility, and reduced total cost of ownership. Contrarily to traditional onsite application architecture where applications are residing in client machines or in a server accessible via client cloud computing offers shared computer application resources and accessible via the Internet.

Since cloud computing share distributed resources via the network in the open environment, it presents an added level of risk because essential services are often outsourced to a third party, which makes it harder to maintain data security and privacy, support data and service availability, and demonstrate compliance. Various categories of such security concerns are trust, architecture, identity management, software isolation, data protection, confidentiality and availability. All these security vulnerabilities lead to various threats on the cloud such as authentication, misuse of cloud infrastructure, eavesdropping, network intrusion, denial of service attack, session hijacking. Further Cloud Forensic is an emerging challenge related to cloud security. It examines the key security issues of Cloud computing being faced today and the challenges and opportunities that it brings for business community. This research paper illustrates a brief description of what exactly cloud computing security-related issues are, and discusses data security and privacy protection issues associated with cloud computing across all stages of data life cycle. It also shows current solutions for data security and privacy protection issues in cloud and describes future research work.

5. On The Impossibility Of Cryptography Alone For Privacy Preserving Cloud Computing

Cloud computing denotes an architectural shift toward thin clients and conveniently centralized provision of computing resources. Clients' lack of direct resource control in the cloud prompts concern about the potential for data privacy violations, particularly abuse or leakage of sensitive information by service providers. Cryptography is an oft-touted remedy. Among its most powerful primitives is fully homomorphic encryption (FHE), dubbed by some the field's "Holy Grail," and recently realized as a

fully functional construct with seeming promise for cloud privacy. We argue that cryptography alone can't enforce the privacy demanded by common cloud computing services, even with such powerful tools as FHE. We formally define a hierarchy of natural classes of private cloud applications, and show that no cryptographic protocol can implement those classes where data is shared among clients. We posit that users of cloud services will also need to rely on other forms of privacy enforcement, such as tamperproof hardware, distributed computing, and complex trust ecosystems.

6. Modeling user search behavior for masquerade detection

Masquerade attacks are a common security problem that is a consequence of identity theft. This paper extends prior work by modeling user search behavior to detect deviations indicating a masquerade attack. We hypothesize that each individual user knows their own file system well enough to search in a limited, targeted and unique fashion in order to find information germane to their current task. Masqueraders, on the other hand, will likely not know the file system and layout of another user's desktop, and would likely search more extensively and broadly in a manner that is different than the victim user being impersonated. We identify actions linked to search and information access activities, and use them to build user models. The experimental results show that modeling search behavior reliably detects all masqueraders with a very low false positive rate of 1.1%, far better than prior published results. 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.

7. Decoy document deployment for effective masquerade attack detection

Masquerade attacks pose a grave security problem that is a consequence of identity theft. Detecting masqueraders is very hard. Prior work has focused on profiling legitimate user behavior and detecting deviations from that normal behavior that could potentially signal an ongoing masquerade attack. Such approaches suffer from high false positive rates. Other work investigated the use of trap-based

mechanisms as a means for detecting insider attacks in general. In this paper, we investigate 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.

8. Technique for Isolation of Malicious Nodes from the Cloud Computing

The cloud computing is the architecture in which virtual machine, cloudlets, and data centers are involved in communication. 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, 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.

9. A New Trusted and Collaborative Agent Based Approach for Ensuring Cloud Security

In order to determine the user's trust is a growing concern for ensuring privacy and security in a cloud computing environment. In cloud, user's data is stored in one or more remote server(s) which poses more security challenges for the system. One of the most important concerns is to protect user's sensitive information from other users and hackers that may cause data leakage in cloud storage. Having this security challenge in mind, this paper focuses on the development of a more secure cloud environment, to determine the trust of the service requesting authorities by using a novel VM (Virtual Machine) monitoring system. The framework can be used to provide security in network, infrastructure, as well as data storage in a heterogeneous cloud platform. If the trust updating policy is based on network activities, then the framework can provide network security. Similarly, it provides storage security by monitoring unauthorized access activities by the Cloud Service Users (CSU). Infrastructure security can be

provided by monitoring the use of privileged instructions within the isolated VMs. The uniqueness of the proposed security solution lies in the fact that it ensures security and privacy both at the service provider level as well as at the user level in a cloud environment.

10. Analysis of Insiders Attack Mitigation Strategies

Insider threat has become a serious information security issues within organizations. In this paper, we analyze the problem of insider threats with emphases on the Cloud computing platform. Security is one of the major anxieties when planning to adopt the Cloud. This paper will contribute towards the conception of mitigation strategies that can be relied on to solve the malicious insider threats. While Cloud computing relieves organizations from the burden of the data management and storage costs, security in general and the malicious insider threats in particular is the main concern in cloud environments. We will analyses the existing mitigation strategies to reduce malicious insiders threats in Cloud computing.

IV. SYSTEM ANALYSIS

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

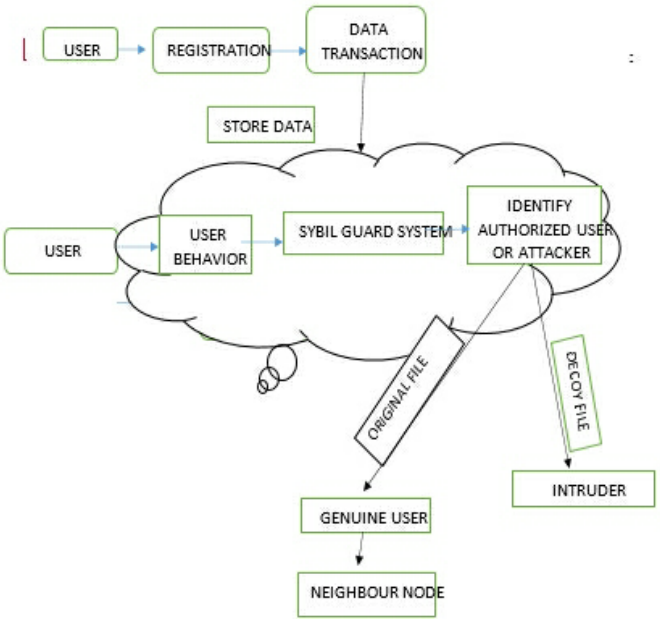
identity of the intruders, instead of that, they focus only on the key provided by the users at the time of accessing the available resources which may or may not provide by the authenticated user.

PROPOSED SYSTEM:

A new methodology which identifies malicious intruders on monitoring the abnormal access patterns through User Behavioral Profile Mapping with the help of data mining algorithms and map reduce. Upon the detection of intrusion, we invoke the decoy data to the attacker and the owner has been informed of the unauthorized access. Whenever an intruder tries to access the data of owner, our system will detect an abnormal pattern of the data access and consequently creates a decoy file with the same filename by scrambling down the real content of the file to an intruder with bogus information.

We monitored the data access over the cloud and try to detect the abnormal access pattern over the cloud. Into this system whenever an intruder try 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 look genuine as the targeted file and provide the same to the intruder.

V. SYSTEM DESIGN



VI. 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 an illegal 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.

VII. REFERENCES

[1] Cloud Security Alliance, Top Threat to Cloud Computing V1.0, March 2010.Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[2] Prevention Of Malicious Insider In The Cloud Using Decoy Documents by S. Muqtyar Ahmed, P. Namratha, C. Nagesh

[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. ManeeshShrivastava

[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 InternationalConference 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, ser. 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] 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. DIMVA11. Berlin, Heidelberg: Springer-Verlag, 2011.

[13] Giuseppe Ateniese, Randal

Burnst Reza Curtmola, Joseph Herringt Lea Kissner, Zachary Petersont Dawn Song, Provable Data Possession at Untrusted Stores.

[14] KomalJeetKaur , 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 -22083.

[15] Fog Computing: Mitigating Insider Data Theft Attacks in The Cloud.

[16] 13. 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. HotSec10. Berkeley, CA, USA: USENIX Association, 2010, pp. 18.

[17] 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. 854867, May 2012.

[18] 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. 129134.

[19] 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: SpringerVerlag, 2011, pp. 181200.

[20] 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. DIMVA11. Berlin, Heidelberg: Springer-Verlag, 2011 International Conference on Inventive Communication and Computational Technologies (ICICCT 2017).