IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud

Ms. Regulavalasa Deekya*[1], Mr. K. Venkatesh Babu*[2]

[1]MCA Student, Department of Master of Computer Applications,
Vignan's Institute of Information Technology(A), Beside VSEZ,Duvvada,Vadlapudi Post,
Gajuwaka, Visakhapatnam-530049.
[2]Assistant Professor, Department of Information Technology,
Vignan's Institute of Information Technology(A), Beside VSEZ,Duvvada,Vadlapudi Post,
Gajuwaka, Visakhapatnam-530049.
vignaniit.edu.in

Abstract:

Cloud computing significantly alters the way we use computers and guarantees access and storage of our personal and business information. These new computing and communication models face new data security challenges. Existing data conservation procedures such as encryption fail to prevent data from the attacks of theft, especially in the cloud provider. So to overcome these problems we are proposing a new technology called Fog Computing. We propose a different approach in Fog computing to obtain data in the cloud using aggressive decoy technology and user behavior profiling. The users using the Cloud are trapped and their access patterns are recorded. Every User has a unique profile which is monitored and updated. We monitor data access in the cloud by the users and detect abnormal data entry patterns. When unauthorized access is suspected and challenged by challenge questions, we begin the wrong attack by returning the bulk of the information to the attacker. This protects users' real data from being misused. Experiments in a local file setting give evidence that this approach can provide an unprecedented level of user security in the cloud environment.

Keywords: Cloud Computing,Fog Computing,Data Security,Abnormal Data.

1. INTRODUCTION

In the ever-evolving landscape of technology, businesses, particularly startups and small to medium businesses (SMBs), are increasingly turning to cloud-based solutions to optimize their data storage and computational needs. While this shift enhances operational efficiency, it simultaneously introduces heightened security risks, with data theft attacks emerging as one of the gravest concerns. The severity of these attacks escalates when the threat actor operates as a malicious insider, posing a significant challenge to the security of cloud computing environments.

Recognizing the growing prominence of insider threats, the Cloud Security Alliance has identified them as a top risk in cloud computing. Despite the awareness among cloud computing customers regarding the potential for data theft, they often find themselves reliant on trust in their service providers for safeguarding critical data. The inherent lack of transparency and control over authentication, authorization, and audit controls within the cloud provider's infrastructure further compounds the vulnerability to insider threats.

In response to these challenges, we propose a paradigm shift in cloud security through the innovative concept of Fog computing. This approach leverages decoy information technology to counteract data theft attempts by malicious insiders. By deploying disinformation attacks, Fog computing aims to confound and impede unauthorized access, making it challenging for malevolent insiders to distinguish genuine sensitive customer data from strategically placed decoys. This proactive strategy not only introduces an additional layer of defense but also disrupts the tactics employed by insider threats, thereby bolstering the overall security posture of cloud-based systems.

2. LITERATURE SURVEY

Traditional data protection mechanisms such as encryption was failed in securing the data from the hackers and attackers. Existing data protection mechanisams does not verify whether the user was authorized or not. Cloud computing security does not focus on ways of the data from unauthorized access. Encryption does not provide much security to user’s personal data or business data.Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy n company strength. Once these things r satisfied, ten next steps are to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior

Salvatore J.S et al [9] proposed a new technology and named it as Fog computing. They implemented security by using decoy information technology. They discussed two techniques, namely User behavior profiling and Decoy technology. In User behavior profiling they checked how, when and how much amount of data and information a user is accessing. They monitored their user‘s activity to check for any abnormality in the data access & usages behavior of the user. The second technology is decoy in which information which is bogus or one can say fake such as honey pots, honey files etc. are used to confuse the malicious intruder or attacker by depicting the information in such a way that it seems real.

Van Dijk et al in [7] 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

Salem B et al in [11] 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 trapbased 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 deploymentrelated 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.

Rocha F et al in [6] 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**.**

J. Pepitone et al [8], proposed highlights of password hacker methods. To launch prevention from disinformation attacks, malicious insiders and a real sensitive customer data is using fog computing. In the cloud data access is monitored and detects abnormal cases. For the attacker we provided large amount of decoy information to mislead them. So that, this can avoids misuse of original data of user. we propose two ways of using Fog computing to prevent attacks such as the Twitter attack, by deploying decoy information within the Cloud by the Cloud service customer and within personal online social networking profiles by individual users.

3. EXISTING SYSTEM

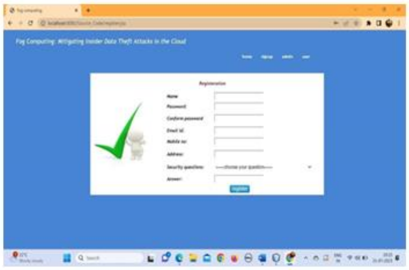
Cloud computing promises to significantly change the way we use computers and access and store our personal and business information. With these new computing and communications paradigms arise new data security challenges. Existing data protection mechanisms such as encryption have failed in preventing data theft attacks, especially those perpetrated by an insider to the cloud provider. Much research in Cloud computing security has focused on ways of preventing unauthorized and illegitimate access to data by developing sophisticated access control and encryption mechanisms. However, these mechanisms have not been able to prevent data compromise.

4. PROPOSED SYSTEM

We propose a different approach for securing data in the cloud using offensive decoy technology. We monitor data access in the cloud and detect abnormal data access patterns. When unauthorized access is suspected and then verified using challenge questions, we launch a disinformation attack by returning large amounts of decoy information to the attacker. This protects against the misuse of the user's real data. Experiments conducted in a local file setting provide evidence that this approach may provide unprecedented levels of user data security in a Cloud environment. We propose a completely different approach to securing the cloud using decoy information technology, that we have come to call Fog computing. We use this technology to launch disinformation attacks against malicious insiders, preventing them from distinguishing the real sensitive customer data from fake worthless data

5. EXPERIMENTAL RESULTS

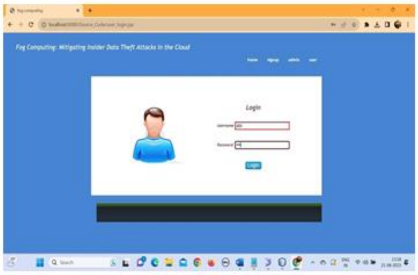
From the below figures it can be seen that proposed model is more accurate in order to prove our proposed system.



Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud

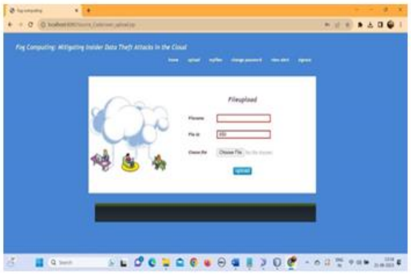
Registration

Name
Password
Conform password
Email id
Mobile no
Address
Security questions —choose your question—
Answer



Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud

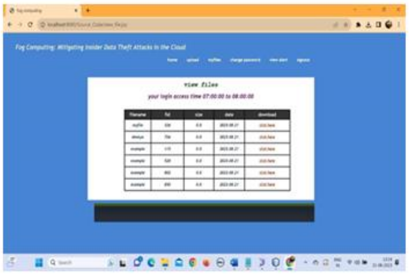
Login



Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud

Fileupload

Filename
File id
Choose file Choose File



Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud

view files

your login access time 07:00:00 to 08:00:00

Filename	fid	size	date	download
myfile	[illegible]	[illegible]	[illegible]	click here
[illegible]	[illegible]	[illegible]	[illegible]	click here
example	[illegible]	[illegible]	[illegible]	click here
example	[illegible]	[illegible]	[illegible]	click here
example	[illegible]	[illegible]	[illegible]	click here
example	[illegible]	[illegible]	[illegible]	click here

6. CONCLUSION

We present a novel approach to securing personal and business data in the Cloud. We propose monitoring data access patterns by profiling user behavior to determine if and when a malicious insider illegitimately accesses someone's documents in a Cloud service. Decoy documents stored in the Cloud alongside the user's real data also serve as sensors to detect illegitimate access. Once unauthorized data access or exposure is suspected, and later verified, with challenge questions for instance, we inundate the malicious insider with bogus information in order to dilute the user's real data. Such preventive attacks that rely on disinformation technology ,could provide unprecedented levels of security in the Cloud and in social networks.

References

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

[2] M. Arrington, "In our inbox: Hundreds of confidential Twitter documents," July 2009. [Online]

[3] D. Takahashi, "French hacker who leaked Twitter documents to TechCrunch is busted," March 2010. [Online] [4] D. Danchev, "ZDNET: french hacker gains access to twitter's admin panel," April 2009. [Online]. Available: http://www.zdnet.com/blog/security/french-hacker-gains-access-totwittersadmin-panel/3292

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

[6] F. Rocha and M. Correia, “Lucy in the sky without diamonds: Stealing confidential data in the cloud,” in Proceedings of the First International Workshop on Dependability of Clouds, Data Centers and Virtual Computing Environments, Hong Kong, ser. DCDV ’11, June 2011.

[7] 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. [Online].

[8] J. Pepitone, “Dropbox’s password nightmare highlights cloud risks,” June 2011.

[9] M. Ben-Salem and S. J. Stolfo, “Modeling user search-behavior for masquerade detection,” in Proceedings of the 14th International Symposium on Recent Advances in Intrusion Detection. Heidelberg: Springer, September 2011, pp. 1–20.

[10] B. M. Bowen and S. Hershkop, “Decoy Document Distributor: http://sneakers.cs.columbia.edu/ids/fog/,” 2009. [Online]. Available: [11] 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:

[11] 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.