ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Fog Computing: Establish Data Security in Cloud

Kiran G. Dhapodkar, Prof.Kahkashan Siddavatam

M.E. Student, Dept. of C.E., LTCOE, Mumbai University, Maharashtra, India

Professor, Dept. of C.E., LTCOE, Mumbai University, Maharashtra, India

ABSTRACT: Cloud computing has changed the way computing takes place significantly. It is a new computing model which enables parties to make use of its services such as Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS) in pay per use. Cloud computing is very important unit in the online world. 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. Using these technologies we detect the behavior of the user and compare it with the normal user behaviour. We are proposing a new technology called as fog computing. Fog computing securing data in the cloud using offensive decoy technology and user behavior profiling. We monitor data access in the cloud and detect abnormal data access patterns. When the application suspects unauthorized access it throws challenges besides launching disinformation attack using decoy information. This Prevents insider theft. If we want to detect the unauthorized user then we can also do that. This protects against the misuse of the user's real data. We want to study the behavior of attacker. Experiments conducted in a local file setting provide evidence that this approach may provide unprecedented levels of user data security in a Cloud environment. Thus provides higher levels of security to the cloud.

KEYWORDS: HMAC-Hashed Mac Authentication Code, Data storage, decoys behavior profiling, cryptographic protocols, cloud computing.

I. INTRODUCTION

Cloud now-a-days forms a basic need of all the firms or organizations that deal with storing of large amount of data, so most of the firms are opting for cloud. Cloud computing is achieving popularity and gaining attention in business organizations. It offers a variety of services to the users. It is an ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources. Since its inception, cloud computing has integrated capabilities dynamically without any investment in incipient infrastructure, providing training to incipient personnel, or licensing any incipient software. Very common risks now days are data theft attacks. Data theft is considered one of the top threats to cloud computing by the Cloud Security Alliance. There is lack of transparency, problem in data dynamics and security related problem like authorization, authentication, and audit controls. Moreover, if the attacker is an Insider than the chances of data theft increase as the insider may already have some personal information. The common notion of a cloud insider as a rogue administrator of a service provider is discussed, but we also present two additional cloud related insider risks: the insider who exploits a cloud-related vulnerability to steal information from a cloud system, and the insider who uses cloud systems to carry out an attack on an employer's local resource.

To deal with such cases and malicious intruders there are some techniques which are used to secure user data. A new technology called Fog computing is gaining attention of the cloud users nowadays. Salvatore J. Stolfo et al. used it for making disinformation attacks against the malicious intruder or attacker Fog Computing is an extension of Cloud Computing. As in a Cloud, Fog computing also provides data, compute, storage, and application services to end-users. The difference is Fog provides proximity to its end users through dense Geographical distribution and it also supports mobility. Access points or set-up boxes are used as end devices to host services at the network. These end devices are also termed as edge network.

II. INFORMATION SECURITY

Information security is a strategy used to protect information from unauthorized users. The objective to validate the access is authorized or not and if abnormal access is detected than providing the hacker with encrypted or unreadable information. We propose a different approach to securing the cloud utilizing decoy information technology, that we have come to call Fog computing. We utilize this technology to launch disinformation attacks against malevolent insiders, obviating them from distinguishing the authentic sensitive customer data from fake worthless data. Fog Computing deals with two technologies User Behavior Profiling and Decoy Information Technology.

The proposed security mechanism makes use of two concept known as user behavior profiling and decoys. User who access cloud to view their own data and also perform data dynamics are expected to have some specific patterns of usage. Such users are known as normal users. This normal behavior of users is profiled in the first phase. The insider theft attackers generally do not have the behavior of normal user. For this reason they are attracted to use decoy information. As the decoy information is not real data there is no problem when hacker uses it or steals it. However, the navigational patterns of the malicious insider can be compared with the navigational patterns of genuine users. The abnormal behavior has to be suspected. The true user of cloud behaves normally and his activities match the general profile of any such users. When decoy information such as bogus information are introduced into the file system. This will provides a security mechanism that can prevent insider data theft.

When the 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. 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 three additional security features:

(1) Validating whether data access is authorized when abnormal information access is detected, and

(2) Confusing the attacker with bogus information that is by providing decoy documents.

(3) Study the behavior of unauthorized user and detect attacker using IP address and MAC address.

III. PROPOSED SCHEME

In this paper, Fog Computing system is trying to work against the attacker specially malicious insider. Here malicious insider means Insider attacks can be performed by malicious employees at the providers or users site. Malicious insider can access the confidential data of cloud users. A malicious insider can easily obtain passwords, cryptographic keys and files. 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 know how employees are granted access and how this access is monitored or how reports as well as policy compliances are analyzed.

The actual working of the fog computing .In two ways login is done in system that are admin login and user login .When admin login to the system there are again two steps to follow:

Step1: Enter username

Step2: Enter the password.

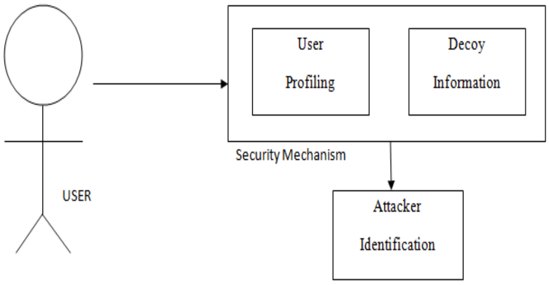


Fig 2: Security Mechanism

After successful login of admin he can perform all admin related tasks, but while downloading any file from fog he have to answer the security Question if he answer it correctly then only original file can be download. In other case ,when admin or user answer incorrectly to the security question then decoy document (fake document) is provided to the fake user . Decoy technology work in the given manner if you have any word ,suppose “MADAM” in the document then some alphabets are replaced as M->A then the given word become “AADAA” which have no meaning. In some Case ,if attacker getting to know that „M‟ is replaced by „A‟ in the given document and by applying reverse engineering he get result as “MMDMM”. In any case he can‟t judge content of document. Fog computing work against the malicious insider attack while this malicious insider attacker can confused with the bogus information. We can also detect the location of the attacker. It will show the attacker IP address and MAC address from which location will attacker use the account.

IV. EVALUATION

Let us consider that we have database ‘D’ and ‘n’ number of attribute such as user name, user id etc.

D = {A|A ε Information of user}

Here D is the set of all A such that A is information of user which is to be store on server

Consider following function

STORE (D, SERVER): Here admin enter the user information into database at server.

Let us consider that the receiver provide us with value “X” for every input it obtain from the every time login account of the particular user .so we can further assume to have a set ‘s to have value ’n’ number of detect value at particular instance.

Let us denote the current situation in the following manner

S = {X| □ X ε D Ǝ ID for attacker}R · e(σγ,g) = e((sc Y i=s1H(Wi)vi)γ · uμ,v). (1)

Suppose that our extractor can rewind a cloud server in the execution of the protocol to the point just before the challenge h(R) is given. Now the extractor sets h(R) to be γ* _= γ. The cloud server outputs {σ, μ*,R} such that the following equation holds.

Here S is the set all X such that for all X there exits Id for user.

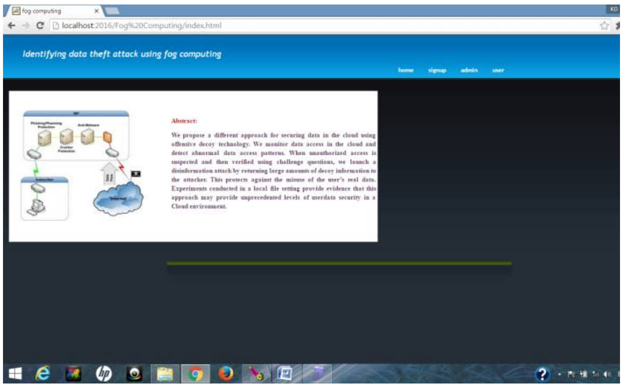
Now, for some X value that match with some value inside the database when admin check user account update.

1. GET(D,X,SERVER): Admin get all information about the user account from server.

2. PUT(X,ATK,SERVER): Here admin will upload attacker’s information on server.

3. PUTP(X,REPORT,SERVER) : Here admin upload daily report on server.

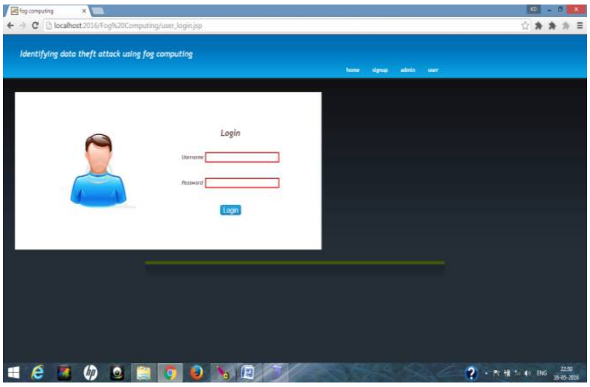
V. EXPERIMENTAL RESULTS


fog computing
localhost:2016/Fog%20Computing/index.html
Identifying data theft attack using fog computing
home
signup
admin
user

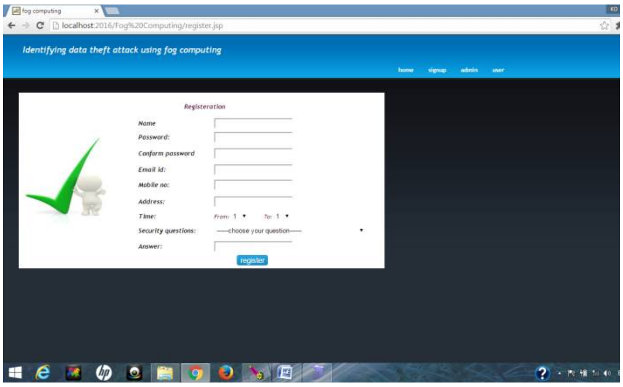
Abstract:

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 userdata security in a Cloud environment.

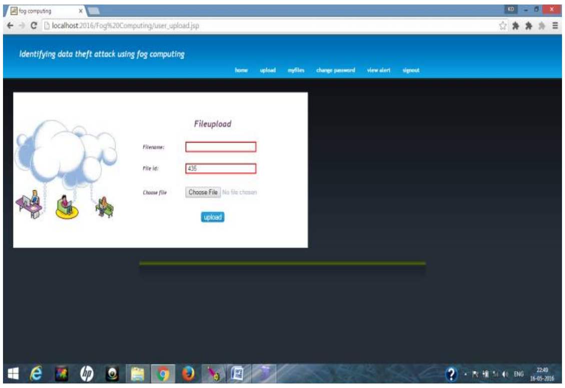
Homepage


fog computing
localhost:2016/Fog%20Computing/user_login.jsp
Identifying data theft attack using fog computing
home
signup
admin
user
Login
Username
Password
Login

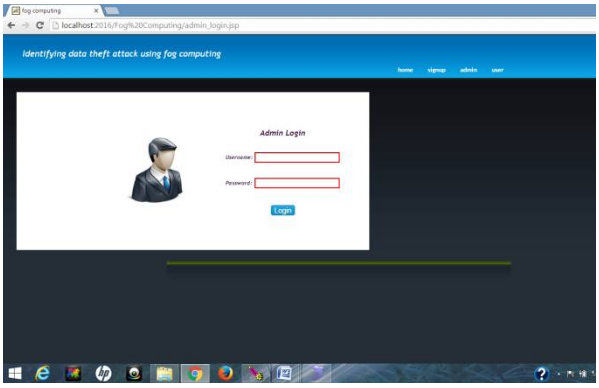
User login page



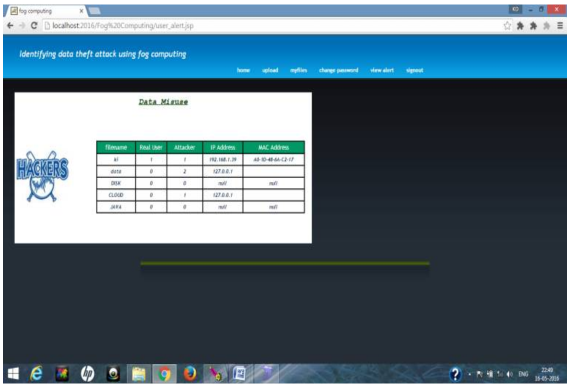
Registration page



File upload page


fog computing
localhost:2016/Fog%20Computing/admin_login.jsp
Identifying data theft attack using fog computing
home
signup
admin
user
Admin Login
Username:
Password:
Login

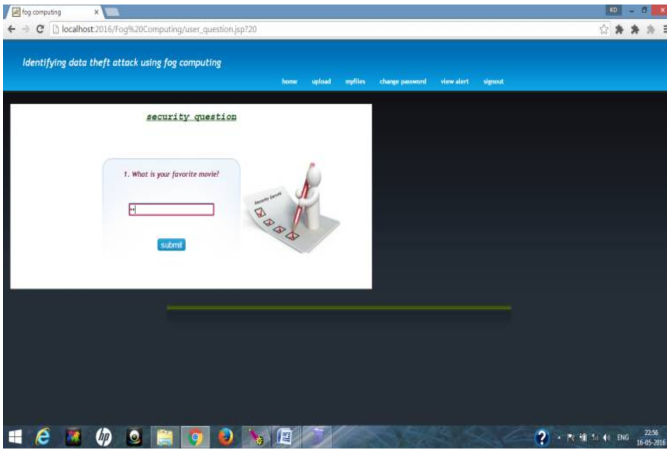
Admin page


fog computing
localhost:2016/Fog%20Computing/user_alert.jsp
Identifying data theft attack using fog computing
home
upload
myfiles
change password
view alert
signout
HACKERS

Data Misuse

filename	Real User	Attacker	IP Address	MAC Address
ki	1	1	192.168.1.39	A0-1D-48-6A-C2-17
data	0	2	127.0.0.1	
DISK	0	0	null	null
CLOUD	0	1	127.0.0.1	
JAVA	0	0	null	null

Data misuse page



Identifying data theft attack using fog computing

security question

1. What is your favorite movie?

Security question page

VI. CONCLUSION

The simulation results showed that the increase of data theft attacks the security of user data security is becoming a serious issue for cloud service providers for which Fog Computing is a paradigm which helps in monitoring the behavior of the user and providing security to the user data. Other techniques discussed in this, use Fog computing for optimizing the website performance. We hope that by continuing this work using Fog Computing platforms can lead to improved defensive techniques and would contribute in increasing the level of security if user data on the cloud. If we want to detect the unauthorized access then by using IP address and MAC address it will be identified. This technology would add up a level in securing the data on the cloud. This paper did not focus decoy information of pertaining to many domains such as banking, insurance, health care and so on. Moreover the user profile management can be improved further to have hierarchy of attributes of user data. These two will be our focus in future work. We would like to enhance the user profile management and use more decoy information from various domains for improving true positives of the fog computing. So by using decoy technique in fog computing can minimize insider attacks in cloud.

REFERENCES

1. Salvatore J. Stolfo, Malek Ben Salem, Angelos D. Keromytis, “Fog Computing Mitigating Inside Data Theft Attacks In The cloud”,IEEE Base Paper, 2013
2. 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.
3. 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,pp. 1–8, 2010.
4. M. Ben-Salem and S. J. Stolfo, “Modeling user searchbehavior for masquerade detection,” in Proceedings of the 14th International Symposiumon Recent Advances in Intrusion Detection. Heidelberg: Springer,pp. 1– 20,September 2011.
5. D. Takahashi, “French hacker who leaked Twitter documents to TechCrunch is busted,” March 2010.S. Wilson, “Appengine outage,” Online at http://www. cio-weblog.com/50226711/appengine outage.php, June 2008.
6. M. A. Shah, R. Swaminathan, and M. Baker, “Privacypreserving audit and extraction of digital contents,” Cryptology ePrint Archive, Report 2008/186, 2008.
7. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, “Enabling public verifiability and data dynamics for storage security in cloud computing,” in Proc. of ESORICS’09, volume 5789 of LNCS. Springer-Verlag, Sep. 2009, pp. 355–370.
8. Cloud Security Alliance, “Security guidance for critical areas of focus in cloud computing,” 2009, http://www. cloudsecurityalliance.org.
9. Y. Dodis, S. P. Vadhan, and D. Wichs, “Proofs of retrievability via hardness amplification,” in TCC, 2009, pp. 109–127.
10. K. D. Bowers, A. Juels, and A. Oprea, “HAIL: A high-availability and integrity layer for cloud storage,” in Proc. of CCS’09, 2009.
11. P. Allen, “Obama’s Twitter password revealed after french hacker arrested for breaking into U.S. president’s account,” March 2010.
12. Cloud Security Alliance, “Top Threat to Cloud Computing V1.0,” March 2010.
13. M. Arrington, “In our inbox: Hundreds of confidential twitter documents,” July 2009.
14. J. Pepitone, “Dropbox’s password nightmare highlights cloud risks,” June 2011

15. B. M. Bowen and S. Hershkop, "Decoy Document Distributor". Ali Ahmad Milad, Hjh Zaiton Muda, Zul Azri Bin Muhamad Noh, Mustafa Almahdi Algaet," Comparative Study of Performance in Cryptography Algorithms" Journal of Computer Science 8 (7): 1191-1197, 2012 ISSN 1549-3636, Malaysia, 2012.

BIOGRAPHY

Kiran Ganpati Dhapodkar is a student in the Lokmanya Tilak College of Engineering, Mumbai University. He received Bachelor of Engineering (B.E) degree in 2013 from BCCE, Nagpur, Maharashtra, India. His research interests are Cloud Computing, Security, Algorithms, etc.