International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 2, February - 2014

Fog Computing using Advanced Security in Cloud

[1.]Rajashri Raut, [2.]Madhuri Waje, [3.]Sayali Kulkarni, [4.]Ajay K. Gupta,
[1,2,3,4.] B.E computer engineering, Institute of Knowledge College of engineering, pune

Abstract--The insider threat remains one of the most vexing problems in computer security. A number of approaches have been proposed to detect nefarious insider actions including user modeling and profiling techniques, policy and access enforcement techniques, and misuse detection .Existing cryptographic data security mechanism such as Encryption has failed in preventing insider data attacks. We propose a different approach for securing data in the cloud using offensive decoy technology.The goal is to confuse and confound an adversary requiring more effort to identify real information from bogus information and provide a means of detecting when an attempt to exploit sensitive information has occurred. "Decoy Documents" are automatically generated and stored on a file system by the D3 System with the aim of enticing a malicious user.

Keywords:Fog Computing , Decoy Technique, Cloud Computing.

I. INTRODUCTION

Cloud computing is a new paradigm which enables ubiquitious,on demand network access to a shared pool of configurable resources with minimal management effort. it provides many services like pay per use model and elasticity of resources. Cloud cannot prevent data theft attacks if they are insider attacks. These attacks have become a serious threat to cloud. Cloud computing customers are well aware of this threat but they are only left with the choice i.e., trusting the service providers. Lack of transparency is one of the reasons for this threat. 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 .Fog computing is an extension of cloud computing. It is a unifying platform at the edge of the network that supports a wide range of emerging applications and services requiring low latency, orchestration of large scale controlled systems, mobility support etc. While this particular attack was launched by an outsider, stealing a customer's admin passwords is much easier if perpetrated by a malicious insider. Many proposals have been made to secure remote data in the Cloud using encryption and standard access controls. It is fair to say all of the standard approaches have been demonstrated to fail from time to time for a variety of reasons, including insider attacks, mis-configured services, faulty implementations, buggy code, and the creative construction of effective and sophisticated attacks not envisioned by the implementers of security procedures. Building a trustworthy cloud computing environment is not enough, because accidents continue to happen, and when they do, and information gets lost, there is no way to get it back.

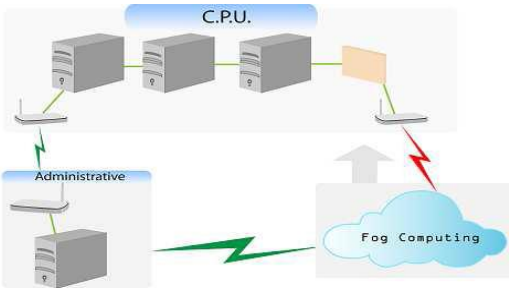

Figure 1. System Architecture

II. FOG COMPUTING

Fog Computing refers to the creation of bogus, "decoy" information placed in the cloud along with otherwise true information to hide what is true from what is bogus. This strategy provides a "fog" of misinformation to protect your sensitive,real information in the cloud! This site was developed by the Columbia Insider Project as a proof-of-concept system that is part of a project on Insider Threat and Attack Detection. Users of this site may download a number of "decoy documents" to be placed on their hard drives as bait to detect and defend against insiders who may gain illegitimate access to a host and steal information. The insider may be human, or a trojan malware program planted to steal credit cards, or logins to online banking or other credentials from the user. Users must first register with the FOG site before they can request and download decoy documents.

Two additional features can be implemented to secure cloud services:

A. User Behavior Profiling

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' behavior 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. This technique usually observes the users search

behavior's it can easily differentiate between normal user and unauthorized user. This method is generally used in fraud detection applications.

B. Decoys

Decoy information such as decoy documents provides bogus information on unauthorized access. Traditional data loss prevention solutions are typically designed to block the unauthorized transmission or copying of documents that contain confidential information. In contrast, decoy documents are created so that they appear to contain sensitive or confidential data. When unauthorized users seeking that type of information come across the decoys and try to open them, they will trip the alarm. Whenever abnormal access to a cloud service is noticed, decoy information may be returned by the Cloud and delivered in such a way as to appear completely legitimate and normal. The true 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 inaccurately detected an unauthorized access. We placed traps within the file system. The traps are decoy files downloaded from a Fog Computing site, an automated service that offers several types of decoy documents such as tax return forms, medical records, credit card statements, e-bay receipts, etc. The decoy files are downloaded by the legitimate user and placed in highly-conspicuous locations that are not likely to cause any interference with the normal user activities on the system.

Decoy serves two purposes:

1. Validating whether the data is authorized and
2. Misleading the user with false or bogus information

III. GENERATION OF DECOY

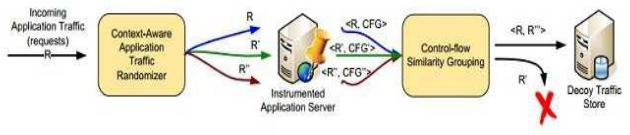

Figure 2. Generation of decoy

The key challenge in generating decoy traffic is that it should appear realistic and indistinguishable from actual user generated traffic. Our goal is for decoy requests to carry the same properties as the actual user input and make the server to behave in the same way. We assume that actual and decoy computation on an application replica is the same as long as, given a real and a corresponding decoy request, similar or identical code execution paths are followed. Currently, we do not place any context-related constraints (e.g. a series of valid protocol messages or application requests that a user would be unlikely to perform in a specific order) as we assume that an attacker would not attempt to distinguish decoys in such manner. However, our approach can be extended to include more decoy evaluation heuristics. Figure presents the process of generating realistic computational decoys. Decoy generation begins with a set of templates for protocol messages generated by popular client applications (e.g. web browsers).Templates are used to generate random permutations in the acceptable value space for the parameters or content of a given message type. For instance, if the message is an HTTP GET request carrying the PIN parameter with a space of four numeric characters the system would generate all permutations.Alternatively, for a search word parameter with a space defined by a dictionary of the English language we would generate an appropriate number of decoys or enough realistic decoys to satisfy a given quota. The system then evaluates all generated decoys against the actual user input from a training set using the heuristics mentioned above. Decoy messages that exhibit similar or identical application server behavior are kept, while the rest are discarded. As dynamic binary instrumentation is computationally expensive, we make a time space trade-off and store the produced decoys for future use rather than carry out real-time generation and evaluation.

IV. COMBINING USER SEARCH MODELING AND DECOY TECHNOLOGY FOR MASQUERADE DETECTION

We have applied these concepts to detect illegitimate data access to data stored on a local file system by masqueraders, i.e. attackers who impersonate legitimate users after stealing their credentials. Only the authorized users could identify this decoy whereas the attackers get confused. They get lots of false information. Both the techniques provide very good security for the true confidential data. Through this the cloud becomes more trustworthy. Detecting abnormal search and decoy traps together may make a very effective masquerade detection system. Combining the two techniques improves detection accuracy.

V. PROPOSED APPROACH

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 users 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.

VI. FUTURE SCOPE

Image, pictures, video can be converted into decoy document. Innovative services and applications to be supported by the Fog.

VII. CONCLUSION

Malicious attacks have become a serious threat to cloud computing. In this paper we have presented an integrated approach to prevent such attacks. Decoy documents which are stored in the cloud alongside the user's real data serve as sensors to detect illegitimate access. 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 model.

REFERENCES

[1] Salvatore J. Stolfo, Malek Ben Salem, Angelos D. Keromytis, Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud, IEEE symposium on security and privacy workshop (SPW) year 2012

[2] Brian M. Bowen, Shlomo Hershkop, Angelos D. Keromytis, Salvatore J. Stolfo, Baiting Inside Attackers Using Decoy Documents, Department of Computer Science, Columbia University,New York, NY 10027

[3] Malek Ben Salem and Salvatore J. Stolfo, Decoy Document Deployment for E_ective Masquerade Attack Detection, Computer Science Department,Columbia University New York, New York 10027, USA.

[4] Flavio Bonomi, Rodolfo Milito, Jiang Zhu, Sateesh Addepalli, Fog Computing and Its Role in the Internet of Things, 170 W Tasman Dr. San Jose, CA 95134, USA

[5] Madhusri.K,Navneet.Y,Harish.CH,Sandeep.A,Dr.T.V.Rao,Fog Computing:Detecting Malicious Attacks in a cloud International Journal of Scientific and Engineering Research,Volume 4, Issue 5, May-2013 1248 ISSN 2229-5518

[6] Jonathan Voris, Jill Jermyn, Angelos D. Keromytis, and Salvatore J. Stolfo, Bait and Snitch: Defending Computer Systems with Decoys, Department of Computer Science, Columbia University, New York, NY 10027.

[7] D. Danchev, ZDNET: French hacker gains access to twitters admin panel, April 2009

[8] P. Allen, Obama s Twitter password revealed after French hacker arrested for breaking into U.S. presidents account, March 2010

[9] 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

[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