ABHIYANTRIKI
An International Journal of Engineering & Technology
(A Peer Reviewed & Indexed Journal)
Vol. 3, No. 5 (May, 2016) http://www.aijet.in/ eISSN: 2394-627X

Decoy Technology: An Attribute based Auditing in Cloud

Pooja N. Nayak*
Student
Deptt. of Computer Science & Engineering
RNS Institute of Technology, Bangalore, India

Shashidhar H. R.
Professor
Deptt. of Computer Science & Engineering
RNS Institute of Technology, Bangalore, India

Abstract

Distributed computing guarantees to fundamentally change the way individuals use PCs and get to and store their own and business data. With these new figuring and correspondences ideal models emerge new information security challenges. Existing information security instruments, for example, encryption have fizzled in forestalling information burglary assaults, particularly those executed by an insider to the cloud supplier. Much research in cloud processing security has concentrated on methods for counteracting unapproved and illegitimate access to information by creating modern access control and encryption systems. However these systems have not possessed the capacity to avoid information trade off. An alternate methodology has been proposed for securing information in the cloud utilizing hostile Decoy innovation. Information access is checked in the cloud and identifies unusual information access designs. At the point when unapproved access is suspected and after that confirmed utilizing challenge questions, it dispatches a disinformation assault by returning a lot of imitation data to the assailant. This secures against the abuse of the client's genuine information.

Keywords*: Cloud computing, Security challenges, Decoy technology, Decoy information.*

****Author for correspondence*** poonyk4u@gmail.com

1. Introduction

Cloud computing provides us a means of accessing the utilities as applications through Internet. The users are provided with on demand resources for their organizations. Although Cloud computing increases the performance and also has some downsides like data theft and various attacks. This enables the intruder for the misuse of data and also interpretation of highly confidential data for illegal purpose. An alternate methodology has been proposed for securing information in the cloud utilizing hostile distraction innovation. Information access is observed in the cloud and identifies unusual information access designs. At the point when unapproved access is suspected and after that checked utilizing challenge questions, it dispatches a disinformation assault by returning a lot of bait data to the aggressor. Tests directed in a neighborhood document setting give confirm that this methodology may give extraordinary levels of client information security in a Cloud situation. This innovation is utilized to dispatch disinformation assaults against vindictive insiders.

The decoy serves two purposes:

a) Validating whether data access is authorized when abnormal information access is detected, and
b) Confusing the attacker with bogus information. So there is a need of decoy technology to protect the sensitive data of user in cloud.

Here, we manages two advancements to dodge unapproved access, they are: User conduct profiling, and Decoy technology. These advancements will help us in distinguishing the unusual conduct of the programmer and giving fake data to keep the information safe from abuse. These innovations will verify the client by login certifications as well as with security addresses that are already set by the client. On the off chance that the accreditations and the security inquiries are not managed legitimately the information gave will be in encoded shape and will be mixed up to the unapproved client.

2. Related Work

The use of deceptive techniques, such as dis-informative propaganda, to thwart one's enemies has played a part in military conflict since antiquity. No one has summarized the importance of dis-information in the context of combat more concisely than Sun Tzu, who wrote that all warfare is based on deception in the Art of War. A well known example of deception in a military context is Operation Bodyguard, which was an allied plan used during World War II to distract German forces from the invasion of Normandy [8]. Although deception is an ancient concept, it has only recently been applied to the process of securing computer systems. Cliff Stoll was the first person known to utilize misdirection in order to secure a network of computers. Stoll established a spurious set of computing resources in order to catch hackers who were attempting to ex-filtrate information from Lawrence Berkeley National Laboratory [6]. This experiment confirmed the ability of decoys to detect attacks. It also identified several tradeoffs between decoy attributes that can be optimized to defend against specific types of attackers. Furthermore, these authors suggested techniques that can be used to increase the attractiveness of decoys to insiders without interfering with the expected workflow of legitimate users [12]. Most recently, the authors of [8] discussed how language manipulation can be used to craft decoy content that adversaries may find more appealing but normal users would be capable of immediately recognizing as fake. Researchers have also begun investigating how the decoy concept can be applied to other domains. For example, in [11], Park and Stolfo develop a system for protecting software repositories by using decoy Java programs to confuse potential thieves.

3. Problem Statement

Numerous cloud administration suppliers are giving stockpiling mists. When you sign into your record, you can transfer, download, erase you can do any operation. Every one of the operations will be done without realizing that whether the client is approved or aggressor. On the off chance that assailant sign into honest client by taking the client name and secret key there is no assurance for delicate information all things considered. There is no security gave to clients information other than encryption system. There are encryption strategies to transmit the information safely over the system however they can't stop the information access if client name and secret key are stolen. Security ought to be given to clients' information even client names and passwords are stolen. To conquer this issue, there is a need of multi-level security. Despite the fact that there is Mobile confirmation method and E-mail check procedure to approve the information get to, those strategies are basically leaving the aggressors. Thus, they are returning again with another method to assault. To decrease the assaults or to execute the assets of aggressor, some more security conventions should be actualized.

Advantages

Providing a multi-level security in the form of Mobile verification, E-mail verification and challenging questions and instead of simply leaving the attacker, we will try to kill his resources by providing the Decoy information when the data access is not validated. Such a technique will provide more security and confuse or divert the attacker with bogus information. Implementing this technique in Cloud Services improves the security over the important information stored by the innocent user.

Disadvantages

User profiling is a surely understood technique that can be connected here to model how, when, and how much a client gets to their data in the Cloud. In any case, keeping information of tremendous number of clients past data, for all intents and purposes does not work.

4. Architecture

Mitigating security risk is well suited for the geographical distribution of resources instead of having a centralized one, meaning Mitigating mist computing is the extension of Cloud computing. The difference is Mitigating mist 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. In Mitigating mist computing platform multi-tier architecture is used. In first tier there is machine to machine communication and the higher tiers deals with visualization and reporting. The higher tier is represented by the cloud. The architecture is as shown in the fig.1 shown below.

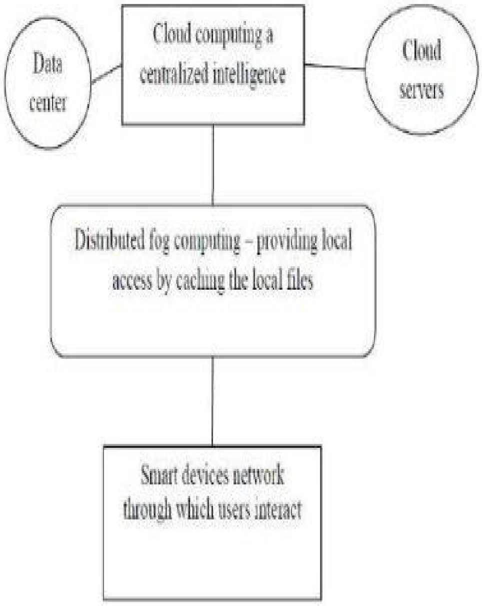
Data center
Cloud computing a centralized intelligence
Cloud servers
Distributed fog computing – providing local access by caching the local files
Smart devices network through which users interact

Fig. 1: Architecture of the system

5. Methodology

Proposed framework is to secure information utilizing hostile distraction innovation. We screen information access in the cloud and identify strange information access designs. At the point when unapproved access is suspected and after that confirmed utilizing challenge questions, we dispatch a disinformation assault by returning a lot of bait data to the assailant. This secures against the abuse of the clients genuine information. This will be rehashed even at the season of downloading from the cloud. Distraction data, for example, bait reports, nectar records, nectar pots, and different fake data can be produced on interest and serve as a method for identifying unapproved access to data and to poison the cheat's ex-filtrated data. Serving imitations will jumble and confound a foe into trusting they have ex-filtrated helpful data, when they have not. This innovation might be coordinated with client conduct profiling innovation to secure a client's data in the Cloud. At whatever point unusual access to a cloud administration is seen, distraction data might be returned by the Cloud and conveyed so as to show up totally real and ordinary.

6. Properties

In this section, the properties of the proposed method are discussed here as:
Believability: One of a decoy's primary functions is to be believable. Upon inspection, a decoy should appear authentic and trustworthy. In the absence of any additional information, it should be impossible to discern a spurious decoy from authentic data. For example, a decoy tax document should contain all of the same fields as one that is actually in use, and each of its fields should be populated with realistic values.

Detectability: The aforementioned decoy properties all concern the relationship between decoy documents and a potential attacker. Detectability, on the other hand, describes the ability of decoys to notify their owner when they have been accessed.

Variability: Although a decoy distribution system should strive to make its fake documents seem as authentic as possible, it would certainly be undesirable if precisely the same well-crafted decoy file were placed repeatedly throughout a given system or network. This would greatly simplify the task of distinguishing between legitimate data and the planted decoys that serve as monitors. In general, there should be as much variability between decoy documents as there exists in the pool of documents that they are intended to detect. That is, the task of identifying a decoy should not be reducible to identifying a particular invariant that exists between all generated decoys.

Differentiability: In effect, the property of decoy non-interference means that true users must be able to easily differentiate between spurious decoy content and authentic data. This can be thought of as the opposite of the believability property. Although decoys should seem as realistic as possible to adversaries, they should appear to be obviously fake for users who should actually be accessing a system. A decoy can be considered fully differentiable if a real user will always succeed at this task.

7. Conclusion

Along these lines in this paper an unmistakable innovation is proposed to make the cloud more secure by securing the individual and the essential information of the business firms. Access to the record is observed by checking the conduct of the client. Access is given by login accreditations as well as by security questions which would be just known not client. To abridge, this paper presented a novel security worldview which allude to as imitation innovation. Baits speak to an intense takeoff from existing security arrangements in a few critical ways. By putting content that is spurious yet conceivable and tempting in the way of potential enemies, imitations can serve as a powerful last line of safeguard against assaults that customary security components neglect to satisfactorily guard against. Fake substance can be proactively seeded all through a framework to guard against potential assaults, or nourished to an enemy once malevolent action has been identified. Moreover, by following distraction material, infringement of classification can be tended to after they have happened. This is ability that option efforts to establish safety are not equipped for advertising.

References

[1] B Bowen, S Hershkop, A Keromytis, & S Stolfo. (2009). Baiting Inside Attackers using Decoy Documents. *In:* Conference on Security and Privacy in Communication Networks, 2009.

[2] B Katz. (2012). Chinese Man Pleads Guilty to NY Fed Cyber. http://www.reuters.com/article/2012/05/29/usacrim e-fedidUSL1E8G TBG120120529

[3] BM Bowen, P Prabhu, V Kemerlis, S Sidiroglou, AD Keromytis, & SJ Stolfo. (2010). Botswindler: Tamper resistant injection of believable decoys in vm-based hosts for crimeware detection. *Recent Advances in Intrusion Detection*. pp. 118-137.

[4] BM Bowen, VP Kemerlis, P Prabhu, AD Keromytis, & SJ Stolfo. (2010). Automating the injection of believable decoys to detect snooping. *In:* Proceedings of the 3rd ACM Conference on Wireless Network Security. pp. 81-86.

[5] C Pettey & R Van-der-meulen. (2011). *Gartner Says Security Software Market Grew 7.5 Percent in 2011*.

[6] C Stoll. *The Cuckoo's Egg*, 1989.

[7] *Columbia University Intrusion Detection Systems Lab*. (2012). *FOG Computing*. Available at http://ids.cs.columbia.edu/FOG/

[8] J Voris, N Boggs, & S Stolfo. (2012). Lost in Translation: Improving Deco Documents via Automated Translation. *In:* Workshop on Research for Insider Threat.

[9] J Yuill, M Zappe, D Denning, & F Feer. (2004). Honey files: Deceptive Files for Intrusion Detection. *In:* Workshop on Information Assurance.

[10] AD Keromytis et al. (2012). The MEERKATS cloud security architecture. *In:* 32nd International Conference on Distributed Computing Systems. pp. 446-450.

[11] Y Park, & S Stolfo. (2012). Software Decoys for Insider Threat. *In:* ACM Symposium on Information, Computer and Communications Security.

[12] MB Salem, & S Stolfo. (2011). Decoy Document Deployment for Elective Masquerade Attack Detection. *In:* Conference on Detection of Intrusions and Malware and Vulnerability Assessment.