Review on Fog computing: Reducing Insiders data theft attack in cloud computing

Prof. Pranalini Joshi
Associate Professor, IT Department, DCOER Pune University
emailD:pranalini.ketkar@zealeducation.com

Asavari Smart
PG student, Computer Department DCOER, Pune university
emailD: asavari_smart@yahoo.co.in

Abstract — Cloud computing is now a day in favour of all types of business units. We can access and store all types of application and data in cloud. As it comes up with more facilities, it becomes exhausting to entrust security. Fog computing provides different security approaches than conventional slant like cryptography. By observing actions and reactions of user while accessing the data, we can find the anomalous behaviour. If unauthorised access detected even after going through challenging questions verification, then we can introduce disinformation attack and provide the fake worthless information to attacker. It will be useful to regulate effectiveness of data. Experiments done by author, shows that, this technique may provide extraordinary level of security for data in cloud computing environment. Fog computing is preventive disinformation attack.

Keywords— Insider, User Behaviour Profile, Decoys, Masquerades, Fog computing, Cloud

I. INTRODUCTION

Traditional business applications and platforms are very complicated and expensive. They need a data centre, complex softwares and a team of experts to run them. So cloud computing becomes more and more popular because of its flexibility, cost effectiveness, easy deployment. The Cloud Security Alliance (2009) [1] declares that the "cloud describes the use of a collection of services, applications, information, and infrastructure comprised of pools of compute, network, information, and storage resources. As cloud computing offers so many benefits to businesses, its security and trustworthiness has always been in question. Security is an extremely important requirement for any IT application, as nobody wants their data to be accessed by unauthorized users. There are many cloud security methods available for external threats. The methods available for external attack have not been able to prevent data theft. Van Dijk and Juels have shown that the solutions like encryption and decryption are not sufficient data protection mechanism when used alone by using fully homomorphic encryption. [2] The ability to leave no trace of an attack is the biggest security challenge for this cloud environment. The lack of resources and evidence makes it difficult to find cloud-based cyber attacks. Data theft attack detection is very difficult when attacker is insider. According to the 2011 CyberSecurity Watch Survey conducted on 607 businesses, government executives, professionals and consultants, 21% of cyber-attacks were caused by insiders. 33% of the respondents thought the insider attacks were more costly and damaging to organizations [3].

Insiders may get the credentials of authorized user of by password sniffing or key logger etc for accessing system or network. Rocha and Correia show that it is very easy to steal passwords for a malicious insider of the Cloud service provider [4].Another case can be like insider may attack on system by taking advantage of victim's unwise trust like person leaves terminal open or allowing to use terminal to co-worker can be pose as masquerade attack. So that service provider cannot get idea of an attack on the system because attacker has identity of authorized user. The most common method used to detect masquerade attack is to keep record of user behaviour and to find anomalous behaviour. In this approach, user's actions are profiled to form a baseline of normal behaviours. Salvatore J. Stolfo and Malek Ben Salem proposed a different approach to secure cloud by using decoy information technology that they called as Fog Computing [5].

II. RELATED WORK

Previous work on detection of masquerade attacks was focused on auditing and modeling sequences of user commands including work on command sequences with information about arguments of commands [6, 7]. For detecting abnormal behaviour researcher applied statistical and machine learning algorithms. Maloof and Stephens also applied a user behaviour profiling technique to detect malicious insider activities violating 'Need-to-Know' policy [8]. Previous studies using multi-class training required gathering data from multiple users to train specific profiles of self and non-self for each user [9]. Different classifiers are also used to detect abnormal behaviour. Combination of different classifier can be a better solution to detect masquerades attack [10]. Traditional computer security defences will not be enough. It will take a combination of things like technical defences, intrusion detection systems, process and more, to provide meaningful and powerful protection.

Another framework is to create a feature set for user behaviours on GUI based systems for masquerade attack. They collected real user behaviour data from live systems and extracted parameters to construct feature.

These vectors contain user information such as mouse speed, distance, angles and amount of clicks during a user session. The technique of user identification and masquerade detection as a binary classification problem uses Support Vector Machine (SVM) [11].

Anomaly detection can produce false positives – a user's behaviour is only anomalous because information such as meeting scheduling is not included – and a high meaningless true positive rate – that is, a user's behaviour may be genuinely anomalous, but not in a dangerous way. Bowen et al. proposed an automated system for generating decoy documents [12.13]. The system generated files are from different templates with various themes, such as a health-related information theme, a financial accounts theme, or a tax returns theme.

III. METHOD TO SECURE CLOUD WITH FOG

Cloud services are designed to provide easy and scalable access to applications, resources and services, and are fully managed by a cloud services provider. It also supplies all types of applications like online data storage and backup solutions, Web-based e-mail services, hosted office suites and document collaboration services, database processing, managed technical support services and more. The problem of desirable level of security for confidential data still exists.

Many methods are proposed to secure cloud data by encryption and standard access control but it is found that the methods are not full proof due to variety of reasons. Customer not only requires reliable cloud environment but also a healthy security for data and applications. Recovering the stolen or lost data is not possible. So we must have knowledge to deal with such incidences. If we decrease the value of stolen data by providing decoy documents then we can limit the harm of the system. Salvatore J. Stolfo and Malek Ben Salem propose extra security features are as follows [5]:

1: User Behaviour Profile
2: Decoys

1. User Behaviour Profile:-

"Behavior" of any given user, if defined appropriately, would be very hard to impersonate. Unfortunately, behavior is turning out to be very hard to define. But it seems clear that for the Insider Misuse problem, some way to automatically process user behavior is absolutely necessary. Cloud service provider seems that user accesses data normally, if any malicious insider accesses data from cloud because insider has identity of victim. To detect that illegitimate access the well known technique of User Profiling should be used. Abnormal user can be detected by observing normal user behavior continuously. This behavior may contain volumetric information generally like which document/application/information he/she is accessing and for how many times, at what timings, for what purpose etc. Abnormal search behavior indicates variations from baseline i.e. of normal user behavior. This technique is generally used for fraud detection applications.

An authorized person of the system is friendly with the files or documents located on the system. The search or behavior of that user is likely to be targeted or finite. But masquerader who gets an access to the victim's system can't have an idea about the structure and content of the system. So their search or access can be misdirected or unbounded. According to Salvatore J. Stolfo and Malek Ben Salem, this is possible masquerades attack. Based on these assumptions they developed the model with the help of one class modelling technique named as one class support vector machine. Benefit of one class support vector over two class is it has ability of building classifier without sharing data from other users. The privacy of user data is maintained. Experiments done by them indicate that we could reliably detect masquerade attacks using this approach with a very low false positive rate of 1.12% [14].

2. Decoys:-

Decoy information like decoy documents or honey file or honey pot is placed in the system at the conspicuous location and stored by very enticing names. Illegitimate user feels that he is getting important information which is not the case. Decoys should be easily retrieved in order to maximize the likelihood that an attacker takes the bait. Decoys should not be easily identifiable to an attacker. It will help us to confuse to attacker. This method can be combined with the User behaviour profiling to secure cloud data.

When abnormal behaviour detected, decoy documents can be returned to user in such a way that it should look like normal. An authorized user of the system would easily understand that decoy information is returned by the cloud and therefore they alter the Cloud's responses by different ways, such as challenge questions or to inform the Cloud security system that it has inaccurately detected an unauthorized access. If an unauthorized access is detected correctly then huge amount of bogus information will be provided to the user. With this method, we can achieve couple of benefits, first: unauthorized access is detected and second: we can confuse the attacker by providing worthless information. It

should be taken into consideration that decoy information should not cause any impact on normal user. By monitoring access to decoy information we can detect illegitimate user.

Combining Two Methods:-

Salvatore J. Stolfo and Malek Ben Salem propose that by combining these two techniques, we can achieve highest level of security [5]. No other cloud security mechanism can provide such level of security. They applied this combined technique in local file system and their experimental results suggested that this combining approach will be very useful in cloud.

The combined approach suggests that first to detect abnormal behaviour using user behaviour profiling. Abnormal behaviour can vary from normal user behaviour baseline. Normal user has an idea about the file structure and contents or documentation of the system. So his search is targeted, whatever file or document he wants to access, the location is likely to be known to him. And if not known then he has some behaviour pattern to search data. According to these assumptions, model is prepared to find anomalous behaviour using one class support vector machine. After detecting abnormal behaviour they placed the traps in the system. Traps are the decoys which are downloaded from fog computing site. Decoys can be anything like important transaction reports, receipts of online purchase, credit card statements, medical reports, tax returns forms, fake password etc. These documents are placed in noticeable location. But care is taken that these decoys should not be interfered with normal user. If normal user accesses these files then he or she will get that it is decoy document. And in case of normal user, unknowingly accesses decoy documents then to decide if he is authorized person or not, display set of challenge-response questions that the user must correctly respond to: The answers to these questions are given by the owner of the system during the installation of the system. In reverse way user is attacker then he or she will be in search of sensitive information such as bait information embedded in decoy document. While accessing decoys, attacker feels that he is getting important information but it is not.

Decoy document carry the Keyed- Hash Message Authentication Code (HMAC). This is hidden in the header section of the document. HMAC is computed over the file content using the key which is unique to each user. When these decoys loaded into memory, they calculate HMAC of the document using file content. And by comparing these two HMAC addresses decoy document is decided and alert is generated. In their experiments they do not provide decoy document on demand. Instead, they place decoy document in very conspicuous location by giving attractive names to directories. By doing this they are able to improve accuracy of detection. Combining these two techniques they get very low false positive rate.

IV. CONCLUSION

Cloud security is one of the major important point to be considered in cloud computing. Masquerade or insider is the person who behaves as a normal user by stealing credentials of authorized person. Insider attack is very difficult to diagnose. So the given approaches help to provide the higher and intelligent level of security in terms of insider attacks. The approaches are based on the predefined user behaviours and monitoring as well as profiling it using decoys. In case of abnormal behaviour i.e. insider attack, decoy documents are presented to the user which is actually a bogus information. These decoy documents can also be checked to detect such insider attack. Thus using these approaches the very important and hard to detect attack i.e. insider attack can be handled and the data can be very well secured. The false positive percentage for these approaches is very low.

V. REFERENCES

[1] Cloud Security Alliance (CSA), (2009). Security guidance for critical areas of focus in cloud computing v2.1 Retrieved from Cloud Security Alliance website: http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf

[2] 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]. Available: http://dl.acm.org/citation.cfm?id=1924931.1924934

[3] 2011 CyberSecurity Watch Survey, CERT Coordination Center at Carnegie Mellon University.

[4] F. Rocha and M. Correia, "Lucy in the sky without diamonds: Stealing confdential data in the cloud," in Proceedings of the First International Workshop on Dependability of Clouds, Data Centers and Virtual Com- puting Environments, Hong Kong, ser. DCDV '11, June 2011.

[5] Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud Position Paper Salvatore J. Stolfo Computer Science Department Columbia University New York , NY, USA Email: sal@cs.columbia.edu Malek Ben Salem Cyber Security Laboratory Accenture Technology Labs Reston, VA, USA Email: malek.ben.salem@accenture.com Angelos D. Keromytis Allure Security Technologies New York , NY, USA

[6] M. Schonlau, W. Dumouchel, W. Ju, A. F. Karr, M. Theus, and Y. Vardi. Computer intrusion: Detecting masquerades. Statistical Science, 16:58–74, 2001.

[7] R. A. Maxion and T. N. Townsend. Masquerade detection using truncated command lines. In DSN '02: Proceedings of the 2002 International Conference on Dependable Systems and Networks, pages 219–228. IEEE Computer Society, 2002.

[8] Maloof, M. A., and Stephens, G. D. elicit: A system for detecting insiders who violate need-to-know. In RAID (2007), pp. 146–166.
[9] One-Class Training for Masquerade Detection Ke Wang Salvatore J. Stolfo Computer Science Department,Columbia University 500 West 120th Street, New York, NY, 10027
[10] Is Combining Classifers Better than Selecting the Best One Saso Dzeroski Saso.Dzeroski@ijs.si Bernard Zenko Bernard.Zenko@ijs.si Department of Intelligent Systems, Joˇzef Stefan Institute, Jamova 39, 1000 Ljubljana, Slovenia
[11] Profling Users in GUI Based Systems for Masquerade Detection: Ashish Garg, Ragini Rahalkar, Shambhu Upadhyaya, Kevin Kwiat
[12] Bowen, B., and Hershkop, S. Decoy Document Distributor: http://sneakers.cs.columbia.edu/ids/ruu/dcubed/.
[13] Bowen, B. M., Hershkop, S., Keromytis, A. D., and Stolfo, S. J. Baiting inside attackers using decoy documents. In SecureComm'09: Proceedings of the 5th International ICST Conference on Security and Privacy in Communication Networks (2009).
[14] M. Ben-Salem and S. J. Stolfo, "Modeling user search-behavior for masquerade detection," in Proceedings of the 14th International Sympo- sium on Recent Advances in Intrusion Detection. Heidelberg: Springer, September 2011, pp. 1–20.