A Secure Framework for Mollifying Attacks in Cloud

Y. Lakshmi Kanth [1], Bhaludra Raveendranadh Singh [2], S.Sunanda [3], Moligi Sangeetha [4]

[1] pursuing M.Tech (CSE), [2]Principal, [3] Assistant Professor(CSE), [4]Associate Professor & HOD (CSE)

[1,2,3,4] Visvesvaraya College of Engineering and Technology (VCET), M.P Patelguda, Ibrahimpatnam (M), Ranga Reddy (D)-501510, India

Abstract: **The cloud computing becoming a major platform for storing the data from various organizations, instead of storing their data with them store in the cloud with this reducing the money as well as work load. We use computers to store and access the personal data as well as business information in the cloud. By this new communication and computing pattern new security issues will arise. The present data encryption techniques are not providing security from data hackers to theft the data. Especially those are performed by insider cloud provider.**

We introducing a new technique for providing security in the cloud, that's a decoy technique, means fault data. Always we will watch data access in the cloud, for detecting abnormal data access, when unauthorized user is noticed will ask some security questions for verifying, we will provide a large amount of decoy data to protect the original data from the attackers, Experiments accompanied in a local file setting provide proof that this method may provide unmatched levels of user data security in a Cloud environment.

Keywords: Cloud Computing, decoy, abnormal data, accompanied

1. INTRODUCTION

Business, especially the star up companies, small and medium based companies, day to day increasingly choosing outsourcing data and calculating the data to the cloud, obviously this will support high operational efficiency, but it come great risk, that the data may be attacked by someone for theft.

The attacks are amplified if the attacker is malicious inside the cloud. This is treated as the most threat to data in the cloud. Most cloud computing customers are aware of this threat. They left only with trusting the service provider for protecting their data. The deficiency of clearness into, let alone control over, the Cloud provider's confirmation, audit controls, and authorization only aggravates this threat.

The Twitter incident was one example for data theft attack in the cloud, some twitter corporate files and personal documents were damaged. The customers' accounts include officials like the U.S president Bhrak Obhama account illegally accessed. The attackers illegally access the Twitter administrator password to gain access the details of personal accounts and then post in the Google. This data damage was very important for both, Twitter corporation and account owners.

To the particular attack done by the outsider, thieving a customer admin password is very easy if performed by malicious insider. Some of the authors also described how the cloud customer's private key must be stolen, and how the customers' data might be extracted from the hard after stealing private keys and password. The malicious insider can access tall data of customer without his permission. The customer doesn't mean to detect the unauthorized access.

Lot of researches in cloud computing security has concentrate on ways to preventing unauthorized user to access the original data by developing the best access control and encryption mechanisms. Though these mechanisms not able to preventing the data attackers in the cloud. Juel and Van Dijk have shown that fully homomorphism encryption. Often attacked by the attacks, these are not sophisticated data protection mechanism while using alone.

We are proposing a completely new mechanism to protect the securing the cloud using decoys information technology that we have called up *Fog Computing***.** We use this technology for disinformation from the malicious insider, preventing them by providing fault data instead of providing original data to unauthorized customers. Here we propose two ways of using Fog computing techniques for preventing such as Twitter attack, by deploying decoy information in the cloud by cloud service customer and social network personal profiles of individual users.

2 SECURING CLOUDS WITH FOG

Several proposals for cloud based services is used to store documents, images, files and media in the cloud (remote services), whenever user want to access the data he connect to the internet and access the particular data. Particularly a worried problem before such services

provided a broad accessing permission to the customer need security. The security is user can gain access the data. The problem of providing security to confidential data remains, as of now not provides as user expected level.

Many suggestions have been made for providing security to the remote storage data using encryption methods and many access controls. It is good to say all of the approaches have been described to fail in the timely manner for variation of reasons, containing misconfigured services, insider attackers, faulty implementation, creative construction and bug codes of effective and the sophisticated attacks not planned by the implementers of the security problems. Providing trustworthy environment is not enough, once data is stolen that will not get back, The data will be steal at the time of travelling from location to another location so we have to prevent those type of accidents.

The elementary idea is that we can limit the damage data if decrease the value of the stolen data to the attacker. We can reach this through deception attack. We recommend that secure Cloud services can be fulfilled given two additional security features:

1) User Behavior Profiling: It is estimated that access to a user's information in the Cloud will show an ordinary means of access. User profiling is a famous technique that can be applied here to perfect how, when, and how much a user can access their information in the Cloud. Such normal user behavior can be constantly checked to define whether anomalous access to a user's information is occurring. This technique of behavior-based security is commonly used in transferring the fraud detection applications. That type of profiles would naturally comprise valuable information, how many documents are typically read and how often. These simple user detailed features can assist to detect irregular Cloud access based partially upon the scale and scope of data

2) Decoys: Decoy information such a fault information like decoy document, honey pots, honey files and various other bug information can be generated on demand and means to assist as a means of finding unauthorized access to information and to contagion the crook's ex-filtrated information. Attending decoys will misperceive and confuse an opposition into trusting they have ex-filtrated useful material, when they have not. This expertise may be amalgamated with user behavior summarizing technology to secure a user's information in the Cloud. Whenever irregular access to a cloud service is noticed, decoy information might be given by the Cloud and exposed in such a way as to seem completely appropriate and normal. The authorized user, who is the actual owner of the information, would willingly recognize when decoy information is being accessed by the Cloud, and henceforward could alter the Cloud's answers through a variety of means, such as experiment questions, to notify the Cloud security system that it has imprecisely detected an unauthorized access. If in case where the access is correctly recognized as an unauthorized access, the Cloud (Remote) security system would give infinite amounts of spurious information to the opponent, thus we can securing the user's true data from unauthorized confession. The decoys, then, help in two purposes: (1) Provide authenticating whether data access is authorized when irregular information access is detected, and (2) baffling the attacker with bogus information.

We speculate that the combination of these two cloud security features will provide extraordinary levels of security in the Cloud. There is no existing Cloud security mechanism is available for providing this level of security.

We have implemented these concepts to recognize illegal data access for the data stored on a local file system by masqueraders that is attackers who satirize genuine users after theft their authorizations. One may consider illegal access to Cloud data by a scalawag insider as the mischievous act of a masquerader. Our investigational results on a local file system setting illustrate that merging both techniques can produce well exposure results, and our results recommend that this method may work in a Cloud environment, as the Cloud is envisioned to be as clear to the user as a local file system. In the following we appraisal briefly some of the experimental results accomplished by using this methodology to discover masquerade activity in a local file setting.

A. Decoy Technology and Combining User Behavior Profiling for Masquerade Detection

1) Decoy Technology: We retained setups within the file system. The setups are decoy files downloaded from a Fog computing site, an automatic service that offers numerous types of decoy documents like medical records, tax return forms, e-bay receipts, credit card statements, etc. The decoy files which are placed in the cloud are downloaded by the authentic user and placed in highly-noticeable locations that are not expected to cause any intrusion with the common user activities on the system. A masquerader, who is not aware with the file system and its information, is supposed to access these decoy files, if the persons is to search for sensitive information, such as the lure information inserted in these decoy files. Therefore, observing access to the decoy files should signal masquerade activity in the system. The decoy documents transmit a keyed-Hash Message Verification Code, which is secreted in the header section of the document. The HMAC is computed in the file's contents using a key unique to each user. Whenever a decoy file is loaded into the cloud memory, we need to verify whether the file is a decoy file by computing a HMAC based on all the contents of that document. We will compare it with HMAC embedded within the documentation. If in case the two

HMACs match, that document is supposed a decoy and an alert is delivered.

The benefits of adding decoy files in a file system are threefold: (1) the reorganization of masquerade activity (2) the confusion of the attacker and the additional costs sustained to differentiate real from bogus information, and (3) the restriction effect which, even though tough to measure, plays a important role in precluding masquerade activity by risk-averse attackers.

2) User Behavior Profiling: Authenticated users of a computer system are having awareness with the files which are available on that system. Any search for particular files is expected to be targeted and limited. A masquerader, though, who gets access to the fatality's system illegally, is unlikely, should have the aware with the structure and contents of the file system. Their search is likely to be general and untargeted.

Based on this key estimation, we summarized user search behavior and established user models trained with a one class modeling technique, explicitly one-class support vector machines. The priority of using one-class modeling branches from the capability of building a classifier without having to share data from dissimilar users. The confidentiality of the user and their data is therefore conserved.

We observe for irregular search behaviors that expose deviations from the user standard. According to our guess, such abnormalities signal a prospective masquerade attack. Our previous experiments certified our assumption and exhibits that we could dependably detect all replicated masquerade attacks by using this approach with the very low false positive rate of 1.12%

3) Combining the Two Techniques: The association of search performance anomaly detection with trap-based lure files should provide stronger proof of malfeasance, and consequently improve a detector's accurateness. We assume that finding of irregular search operations performed earlier to an unsuspicious user opening a decoy file will substantiate the suspicion that the user is definitely imitating another victim user. This situation will cover the threat model of prohibited access to the Cloud data. Still, an unintentional opening of a decoy file by a genuine user might be identifying as an accident if the searching performance is not estimated abnormal. In other words, finding irregular search and decoy traps together might be make a very efficient masquerade detection system. The combination of two techniques improves detection exactitude.

We will use the decoys as a revelation for validating the alerts are displayed by the sensor monitoring the user's file quest and access behavior. In our proposed experiment, we couldn't generate the lure files based on demand at the time of finding when the alert was issued. Rather than, we made sure that the decoys were noticeable enough for the attacker to get them if they were definitely trying to theft information by placing them in highly conspicuous encyclopedias and by giving them enticing names. With this methodology, we were capable to improve the accuracy of our detector. Creating the decoys based on situation improves the exactness of the detector even additional. The collection of two techniques and having the decoy documents act as a truth for our detector when an unauthorized user behavior is detected might be lower the overall false positive rate of detector.

We were trained eighteen classifiers with the total computer usage data from those 18 computer science students were collected over a period of 4 days on average. The classifiers were trained by using the search behavior abnormality detection described in a previous paper. We also prepared another 18 classifiers using a detection technique that combining user behavior profiling with observing access to decoy files placed in the local file system, as mentioned above. We tested these classifiers using replicated masquerader data. Figure 1 displays the AUC scores reached by both detection approaches by user model. The consequences shows that the models using the combined discovery approach achieve equal or better results than the search profiling approach alone.

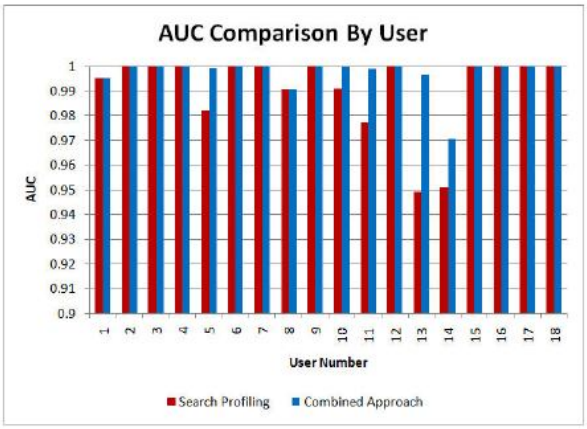


Fig.1. AUC Comparison By User Model for the Search Profiling and Integrated Approaches

The consequences of our experiments propose that user profiles are exact enough to detect unauthorized Cloud access. Whenever such type of unauthorized access is detected, one can respond by giving the user with a respective question or with a decoy document to check whether the access was really illegal, similar to how we will use decoys in a local file setting, to authenticate the alerts delivered by the anomaly detector that monitors user file search and access behavior.

3. CONCLUSION

In this pare, we are describing a novel mechanism to securing the business data and personal data which are

stored in the cloud, we introduce a mechanism to monitor access control with trusted user, for this it uses decoys, along with original file it will stores decoy files. It always check for data accessing once unauthorized user detecting to access the original data, it will display decoy files instead of original data, for this it will ask challenging questions to the user and it will not display any alert message to the user if he is fault user, instead of showing alert message it will display decoy files, Only original user can know about his data, if in case display fault data, by this way we are providing security from the insider attackers.

REFERENCES

[1] Cloud Security Alliance, "Top Threat to Cloud Computing V1.0,"March2010.[Online].Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[2] M. Arrington, "In our inbox: Hundreds of confidential twitter documents," July 2009. [Online]. Available: http://techcrunch.com/2009/07/14/in-our-inbox-hundreds-ofconfidential- twitter-documents/

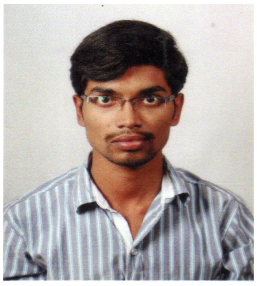
[3] D. Takahashi, "French hacker who leaked Twitter documents to TechCrunch is busted," March 2010. [Online]. Available: http://venturebeat.com/2010/03/24/french-hacker-wholeaked- twitter-documents-to-techcrunch-is-busted/

[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-totwitters- admin-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]. Available: http://www.dailymail.co.uk/news/article-1260488/Barack-Obamas-Twitter-password-revealed-French-hacker arrested.html

[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.

AUTHOR PROFILE



Mr. Y. Lakshmi Kanth is currently pursuing M.Tech in the Department of Computer Science & Engineering, Visvesvaraya College of Engineering and Technology, M.P Patelguda, Ibrahimpatnam (M), Ranga Reddy(D), India. His research interests include Data Security.

Ms. Sandi Sunanda working as Asst. Professor (CSE) in Visvesvaraya College of Engineering and Technology, M.P Patelguda, Ibrahimpatnam (M), Ranga Reddy(D), India.

Ms's. Sangeetha M working as Assoc. Professor & HOD (CSE). She has completed bachelor of technology from Swamy Ramananda Theertha Institute of Science & Technology and Post-graduation from Jawaharlal Nehru Technological University,Kakinada campus and is having 12 years of teaching experience.

Sri Dr. Bhaludra Raveendranadh Singh working as Associate Professor & Principal in Visvesvaraya College of Engineering and Technology obtained M.Tech, Ph.D(CSE)., is a young, decent, dynamic Renowned Educationist and Eminent Academician, has overall 20 years of teaching experience in different capacities. He is a life member of CSI, ISTE and also a member of IEEE (USA)