MIST OPERATION OF COMPUTERS: DETECTING INSIDE INFORMATION STEALING ATTACKS WITH IN THE CLOUD

[1]*T.SHYAM KUMAR*, [2]*M.PAVAN KUMAR*
[1]Associate Professor and HOD-IT, Aurora College, Hyderabad, India.
[2]PG Scholar, Aurora College, Hyderabad, India.

ABSTRACT- *Cloud Computing is a term used to elevate a trend network that depends upon computing that occupies over the Internet for normal usage from Computing Utility, a set or bunch of networked and integrated hardware, Internet infrastructure also known as platform and software. Utilization of Internet for transport and communication of data it gives permission for hardware, software and networking authorities to clients. These platforms will not show the complexity and details of the underlying infrastructure from users and applications by providing very simple graphical interface or API (Applications Programming Interface Cloud computing is a type of the use or operation of computers that relies on sharing computing resources rather than having local servers or personal devices to handle applications. Businesses, especially startups small talks, small and medium businesses (SMBs), are increasingly opting for outsourcing data and the action of mathematical calculation to the Cloud. This will supports better operational the state or quality of being efficient, but comes with higher risks, perhaps the most serious of which are data hacking attacks. Data theft attacks are increase the volume of the attacker is a intended to do harm insider. This is considered as one of the top effective threats to cloud computing by the Cloud privacy Alliance. While most Cloud computing users are well-aware of this effective threat, they are left only with trusting the service provider when it comes to protect their data. The lack of temporary information into, let alone constraints over, the Cloud provider authentication, authorization, and audit controls only make worse with this threat. We are proposing a completely different approach to secure the cloud, using decoy information technology, which is Fog computing. Differencing the valid user and the attacker (the user, who is doing identity crime). With this technology to launch hacking attacks against a intended to do harm insiders, preventing them from differentiating the real sensitive customer data from lure worthless data. Mist Computing is an approach to dismiss unauthorized and illegitimate access to the data with sophisticated access controls. The Lure Information Technology is used for validating whether data access is authorized when abnormal information access is identified. Confusing the attacker with lure information. Lure technology is protecting the real user's sensitive data on the cloud from the attacker (insider data theft attacker).Securing the cloud with decoy information technology and is called as "Mist use operation of computers". The Lure Information Technology is used for Validating whether data access is a real user when unusual information access is detected. Confusing the attacker with wrong information.*

Keywords: Mist, Insider data stealing, Bait information, Lure Files, Validating user, Confusing the attacker.

1. INTRUDUCTION

Platforms will not show the complexity and details of the underlying infrastructure from users and applications by providing very simple graphical interface or API (Applications Programming Interface Cloud computing is a type of the use or operation of computers that relies on sharing computing resources rather than having local servers or personal devices to handle applications.

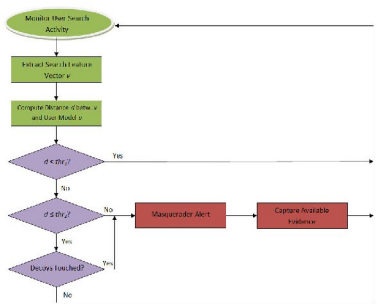
Businesses, especially startups small talks, small and medium businesses (SMBs), are

increasingly opting for outsourcing data and the action of mathematical calculation to the Cloud.
This will supports better operational the state or quality of being efficient, but comes with higher risks, perhaps the most serious of which are data hacking attacks.
Data theft attacks are increase the volume of the attacker is a intended to do harm insider. This is considered as one of the top effective threats to cloud computing by the Cloud privacy Alliance.
While most Cloud computing users are well-aware of this effective threat, they are left only with trusting the service provider when it comes to protect their data.
The lack of temporary information into, let alone constraints over, the Cloud provider authentication, authorization, and audit controls only make worse with this threat.
We are proposing a completely different approach to secure the cloud, using decoy information technology, which is Fog computing.
Differencing the valid user and the attacker (the user, who is doing identity crime).
With this technology to launch hacking attacks against a intended to do harm insiders, preventing them from differentiating the real sensitive customer data from lure worthless data.
Mist Computing is an approach to dismiss unauthorized and illegitimate access to the data with sophisticated access controls.
The Lure Information Technology is used for validating whether data access is authorized when abnormal information access is identified.
Confusing the attacker with lure information.
Lure technology is protecting the real user's sensitive data on the cloud from the attacker (insider data theft attacker).

2. LITERATURE REVIEW

User Behavior Profiling

Most of the prior user behavior profiling work focused on auditing and modeling sequences of user commands including work on enriching command sequences with information about command arguments [28, 21, 32, 22, 20, 11, 26, 25, 35]. A thorough review of these machine learning techniques can be found in this survey [2].
The detection rates of these anomaly detection techniques ranged between 75.8% and 26.8%, with FP rates ranging between 1% and 7%.
These results are obviously far from developers satisfaction. Maloof and Stephens also applied a user behavior profiling technique to detect malicious insider activities which violated `Need-to-Know' policy [19].
In order to identify bad insider behavior, they defined the malicious user scenarios and had to combine results from 76 different sensors through a Bayesian net.
Although the few attack scenarios tested were detected, there was no real evaluation of the FP rate associated with the overall classifier. Finally, Ben-Salem and Stolfo invented a search-behavior profiling approach for detecting masquerade attacks [5]. We focused on modeling user search behavior to reveal an attacker's malicious intent.
A system composed of honey pots and network-level sensors for traffic profiling was proposed by Maybury et al. [23]. The sensors monitored insider activities such as network scanning and file downloads. Pre-specified models of insiders and pre- attack indicators were used to infer the malicious intent of an inclusive insider. However we did not report any test and evaluations. In this paper we integrate host- level user monitoring with honey tokens, as opposed to network-level monitoring that Maybury et al. proposed, and we provide a thorough evaluation of the integrated approach.



2.1 Architecture of the RUU Masquerade Attack Sensor

Normal User Data Collection In order to evaluate the integrated detection approach, we gathered both normal user data and simulated unknown data, that could be used to build user search models and test for abnormal search and access to decoy documents.

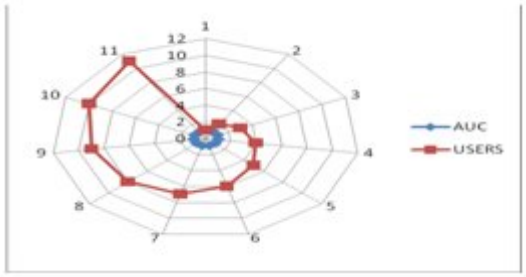
To do so, we conducted two user studies. Eighteen computer science students participated in the first user study. Nine of them placed 20 lure file documents, and nine others placed 30 decoy documents on their local file systems. When placing the bait information files, the students were encouraged to select file locations such that the conspicuousness of the lure files is increased, while the non-influence with user activities is minimized. The participants in this user study also installed a host sensor on their personal machines, which audited their search activity, registry-based activity, process creation and the action or process of causing so much damage to something that it no longer exists or cannot be repaired, window GUI access, DLL libraries activity and lure file document accesses. The data collected by the host sensor were automatically and periodically uploaded to a central server for the analysis.

2.2 Experimental Setup

We used 80% of the data to train one-class SVM models using features as described. We used the LibSVM tool kit to build the models [9]. We also developed a linear bait information access classifier for each user, which checks the previous history of incidental accesses of the user to the lure file documents on their file system. Based on this previous historical behavior pattern, we select a threshold limit, beyond which access to lure file documents is considered excessive or showing a cautious distrust of someone or something, in other words indicative of a false show activity. These models are also developed for each individual user by using 80% of the lure access data. We used the rest of the user data, as well as the showing a careful to avoid potential problems distrust of someone or something a false data for testing the user models.

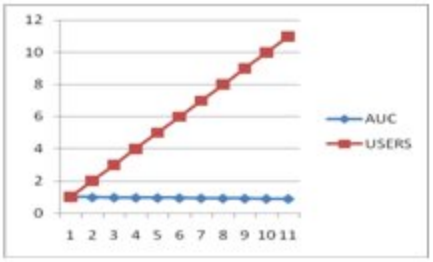
2.2.1 Detection Accuracy

We ran two different mechanisms. In the first mechanism we developed and tested one-class SVM models using the same search profiling approach presented by BenSalem and Stolfo [5]. In the second mechanism we supplemented these models with a linear classifier based on lure file accesses. The below figure displays that using the combined or mixed approach achieves a 99.94% detection rate or TP rate with a 0.79% False positive rate. The TP rate is almost equal to that achieved by the search profiling approach only, while the false positive rate is 36% lower. The False positive rate translates to one false positive every 260 minutes, or every 4 hours and 20 minutes, as opposite to one false positive every 180 minutes or 3 hours. Experimental results of the search profiling and integrated modeling approaches using 2-minute quanta for feature vector extraction Method True Pos. (%) False Pos. (%) Search Profiling 100 1.12. We can further reduce the frequency of false positives to one every 5 and a half hours (338 minutes), if we use the equivalent modeling approach over 5-minute quanta. This is derived from the 1.48 false positives recorded every 5*100=500 minutes, as reported in Table. While this is still a relatively high frequency of false positives, it can be further optimized if we increase the look-ahead time window where we check for decoy access.



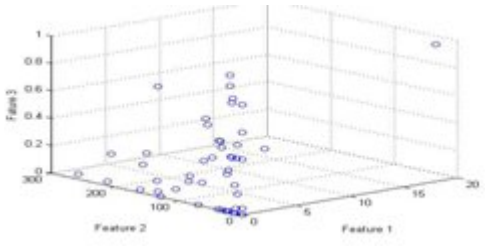
The below figure displays the AUC scores achieved by both detection approaches by user model. The results show that each user model using the combined detection approach achieves a higher or equal AUC score that is equivalent or better accuracy results than the user model based on the search profiling approach alone.

The best accuracy achievements were achieved for users 5, 11, 13 and 14. This user module had the top four FP rates amongst all user models based on search profiling alone. For these specific users, the FP reduction ranged between 33% and 67% when using the combined detection approach. This confirms the efficacy of using this combined approach to limit the number of false positives and improve the accuracy of the masquerade attack detector.

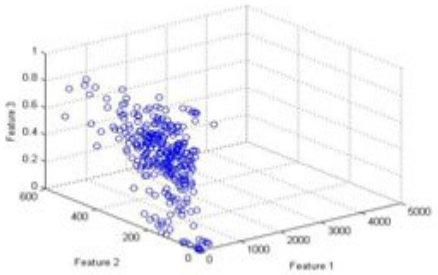


(a) Modeling using feature vectors

(b) Modeling using feature vectors per 5-minute quanta per 2-minute quanta.



(a) Feature Vectors for User 13



(b) Feature Vectors for Masquerade Attackers

3. EXISTING SYSTEM

Encryption or HTTPS secured transactions failed to prevent insider data theft attacks, because of the attacker's has the valid user name and password.

Fog Computing is an approach to prevent unauthorized and illegitimate access to the data with sophisticated access controls.

4. PROPOSED SYSTEM

Securing the cloud with decoy information technology and is called as "Fog Computing".

The Decoy Information Technology is used for Validating whether data access is a real user when unusual information access is detected. Confusing the attacker with lure information.

5. SCOPE OF DEVELOPMENT

Securing the cloud with decoy information technology and is called as "Fog Computing". The Decoy Information Technology is used for Validating whether data access is a real user when unusual information access is detected. Confusing the attacker with wrong information.

User Access Behavior Profiling

It is expected that access to a user's information in the Cloud will exhibit a normal meaning of access. User profiling behavior is a well known mechanism that can be applied here to model how much, when the time of user, and how much a user accesses the data 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 user behavior-based security is commonly used in false user detection applications.

Anomaly Detection

The correlation of search behavior anomaly detection with trap-based decoy files should provide stronger evidence of wrong doing, and therefore improve a detector's speed. We hypothesize that detecting abnormal search operations performed prior to an unsuspecting user opening a lure file will conforming the suspicion that the user is indeed impersonating another victim user. This thing covers the person or thing likely to cause damage model of un-authorized access to Cloud information. Furthermore, an accidental opening of a lure file by a real user might be identified as an accident if the search behavior is not deemed as unusual. In other words, detecting abnormal search and decoy traps together may make a very effective masquerade detection system. Combining the two mechanisms improves detection speed. We use lure as an oracle for validating the alerts issued by the sensor monitoring the user's file search and access behavior. In our mechanisms, we did not generate the lure on demand at the time of detection when the alert was generated. Instead, we made sure that the lure files were clear visible enough for the attacker to access them if they were indeed trying to steal information by placing them in highly conspicuous directories and by giving them attractive names. With this approach, we can able to improve the speed of our detector. The activity of the lure files on demand improves the speed of the detector even further. Combining the two mechanisms, and having the lure documents act as an oracle data base for our detector when an unusual user behavior is detected may lower the overall false positive rate of detector.

6. CONCLUSION

In this position paper, we present a novel approach to securing personal and business data in the Cloud environment. We propose watching the data access patterns by calculating user access pattern to determine if and when a hacker is insider unknowingly accesses someone's documents in a Cloud service environment. Lure file documents stored in the Cloud environment alongside the user's real data also give service as sensors to detect unknown access. Once unknown data access or exposure is suspected, and later verified, with pop up messages given to the user for instance, we overwhelm the hacker insider with lure information in order to dilute the user's real data.

7. REFERENCES

1. [Ben-Salem, M. RUU dataset: http://www1.cs.columbia.edu/ids/RUU/data/.]

2. [Ben-Salem, M., Hershkop, S., and Stolfo, S. J. A survey of insider attack detection research. In Insider Attack and Cyber Security: Beyond the Hacker (2008), Springer.]

3. [Ben-Salem, M., and Stolfo, S. J. Decoy document deployment for effective masquerade attack detection.]

4. [Ben-Salem, M., and Stolfo, S. J. Detecting masqueraders: A comparison of one class bag-of-words user behavior modeling techniques. In MIST '10: Proceedings of the Second International Workshop on Managing Insider Security Threats, Morioka, Iwate, Japan (June 2010), pp. 3{13.]

5. [Ben-Salem, M., and Stolfo, S. J. Modeling user search-behavior for masquerade detection. In Columbia University Computer Science Department, Technical Report # cucs-033-10 (2010).]

6. [Bowen, B., and Hershkop, S. Decoy Document Distributor: http://sneakers.cs.columbia.edu/ids/ruu/dcubed/.]

7. [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).]

8. [CERT. 2010 e-crimes watch survey, 2010.]

9. [Chang, C.-C., and Lin, C.-J. Libsvm: http://www.csie.ntu.edu.tw/ cjlin/libsvm/.]

10. [Cloud Security Alliance, "Top Threat to Cloud Computing V1.0," March 2010. Online. Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf]

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

12. [D. Takahashi, "French hacker who leaked Twitter documents to TechCrunch is usted," March 2010. [Online]. Available: 4
13. [D. Danchev, "ZDNET: french hacker gains access to twitter's admin panel," April 009. [Online]. Available: 4

AUTHORS

T. SHYAM KUMAR is working as Head, Department of Information Technology ASTRA, Hyderabad, India. He has received M.Tech. (Computer Science and Technology) from JNTUH. Presently, he is a Research Scholar of JNTUH Hyderabad. He has published and National Conferences. His main research interests are Software Engineering, Software Metrics, Software Quality.

M. PAVAN KUMAR (M.Tech Scholar) Aurora engineering college (Aurora Bandlaguda) my area of interest and research is in cloud computing. He has published and presented more than 5 Research and technical papers in International Conferences and National Conferences.