© 2019 IJSRSET | Volume 6 | Issue 2 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology
DOI : 10.32628IJSRSET196235

A Review on User Behavior Profiling and Decoy Technology in Cloud Computing

Sonam Satyanarayan Tiwari[1], Prof. Roshani Talmale[2]

[1]M.Tech Scholar, Department of Computer Science and Engineering Tulsiramji Gaikwad-Patil College of Engineering and Technology Nagpur, Maharashtra, India

[2]Department of Computer Science and Engineering Tulsiramji Gaikwad-Patil College of Engineering and Technology Nagpur, Maharashtra, India

ABSTRACT

Now a day's information technology growing vastly to provide users with lots of services but it will lead to security problems. One of them is secret key file. Password files have a great deal of security issue that has influenced a great many clients as well the same number of organizations. Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. Cloud computing significantly modifies the way we use computers and guarantees access and storage of our personal data and business information. These new computing and communication models face new data security challenges. To keep sensitive userdata confidential against untrusted servers, existing solutions usually apply cryptographic methods like encryption by disclosing data decryption keys only to authorized users. But like encryption fail to prevent data from the attacks of theft, especially in the cloud service provider in case key is lost by user or owner. We propose a different approach to overcome these problems in the cloud using decoy technology and user behavior profiling. The users using the Cloud are trapped and their access patterns are recorded. Every User has a unique profile which is monitored and updated. We monitor data access in the cloud by the users and detect abnormal data entry patterns. When unauthorized user try to access or is detected and challenged by challenge questions, we begin the wrong attack by returning the bulk of the information to the attacker. This protects users' real data from being misused.

Keywords : Cloud Computing, Encryption, Security, Decoy Technology, User Profiling Behavior.

I. INTRODUCTION

Cloud Computing(CC) has been stated by NIST as a model forenabling convenient, on-demand network access to a sharedpool of configurable computing resources that can be rapidlyprovisioned and released with minimal management effort or service provider interaction. The CC modelhas three service models and four deploymentmodels. The three service models, also called SPI model. A number of computing resources provided over the internet. Aninternet based computing is an environment where you pay only for resources that you use called as pay as you go. In Cloud we have three parties (Cloud service user, Cloud service provider (CSP) called Cloud user, Cloud provider (CP).CCconcept is rapidly increasing that has a technology connection with Grid Computing, Utility Computing and Distributed Computing. CSP such as Amazon IBM, Google's Application, Microsoft Azure etc., provide theusers in developing applications in cloud environment and to access them from anywhere.

Cloud data are stored and accessed in aremote server with the help of services provided by cloud service providers.

Cloud Services

i. Cloud Software as a Service (SaaS):

Cloud Software as a Service SaaS assures that complete applications are hosted on the internet and users use them. It generally need not to be install and run the application on the customer's local computer, thus alleviating the customer's burden for software maintenance.

ii. Cloud Platform as a Service (PaaS):

In this Paas model of CloudComputing, the CP provides a platform toutilize.Services provided by this model use Application Program Interfaces (APIs), website portals, orgateway software. Buyers do need to look closely at specificsolutions, because some providers do not allow softwarecreated by their customers to be moved off the provider's platform. According to NIST the capability provided to theconsumer is to deploy onto the Cloud infrastructure consumercreatedor acquired applications created using programming.Languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying Cloud infrastructure including network, servers,operating systems, or storage, but has control over thedeployed applications and possibly configuration settings forthe application-hosting environment. Buyers do need to lookclosely at specific solutions, because some providers do notallow software created by their customers to be moved off the provider's platform.

iii. Cloud infrastructure as a service (IaaS):

This is the base layer ofthe Cloud stack. It serves as a foundation for the other twolayers, for their execution. The keyword behind this stack is Virtualization. Usually platform-independent; infrastructure costs are shared and thus reduced; service level agreements(SLAs); pay by usage that is pay as u go model; self-scaling. Avoid capital expenditure on hardware and human resources; reduced ROI risk; low barriers to entry; streamlined and automated scaling but disadvantages are Business efficiency and productivity largely depends on the vendor's capabilities; potentially greater longterm cost; centralization requires new/different security measures. With, a company can rent fundamental computingresources for deploying and running applications or storingdata. IaaS enables fast deployment of applications, andimproves the agility of IT services by instantly addingcomputing processing power and storage capacity when needed.

II. SECURITY AND THE CLOUD

CC infrastructure is, in principle, subject to all of the threats that standard server computing infrastructure is. Web servers can be compromised with cross-site scripting vulnerabilities; databases are subject to SQL injection attacks; operating system kernels can be compromised by machine code injection. Here, however, we are concerned with ways in which cloud-based systems are different from traditional servers from a security perspective.

A Browser attack is committed by sabotaging the signature and encryption during the translation of SOAP messages in between the web browser and web server, causing the browser to consider an adversary as a legitimate user and process all requests communicating with web server.

In addition, if any kind of failure occurs, it is not clear who is the responsible party. A failure can occur for various reasons: 1) due to hardware, which is in the Infrastructure as a Service (IaaS) layer of the cloud; 2) due to malware in software, which is in the Software as a Service (SaaS) layer of the cloud; or 3) due to the

customer's application running some kind of malicious code, the malfunctioning of the customer's applications or a third party invading a client's application by injecting bogus data. Whatever the reason, a failure can result in a dispute between the provider and the clients. From the client point of view, data loss or interruption in computation can cost financially as well as affect a business reputation. From the provider point of view, the quality of service (QoS) is hampered, the SLA is not being satisfied and there can be unnecessary charges to the customers for which the customer is not responsible. These are all costly, affecting the provider's business reputation. Considering the above issues, one of the main focuses of CC is its security.

Cloud computing parties

i) Client:Users access CC using networked client devices, such as desktop computers, laptops, tablets and smart phones. Some of these devices - cloud clients - rely on cloud computing for all or a majority of their applications so as to be essentially useless without it. Examples are thin clients and the browser-based Chrome book.

ii) Application:A cloud application is software provided as a service. It consists of the following: a package of interrelated tasks, the definition of these tasks, and the configuration files, which contain dynamic information about tasks at run-time.

iii) Platform:Cloud platform services, also known as platform as a service (PaaS), deliver a computing platform and/or solution stack as a service, often consuming cloud infrastructure and sustaining cloud applications.

iv) Infrastructure:Cloud infrastructure services, also known as "infrastructure as a service" (IaaS), deliver computer infrastructure typically a platform virtualization environment as a service, along with raw (block) storage and networking.

v) Server:The Layers contain both hardware and software; these are the layers on the server. Products that are specifically designed for the delivery of cloud services, including multi-core processors, cloudspecific operating systems and combined offerings

D. User Behavior Profiling:

User behavior profiling is a popular technology in fog computing which is used to determine when and how frequently the user access his data in the cloud. The way to access Cloud's user information is predictable. This behavior of the user is constantly checked for abnormal activity. Each user has a unique profile consisting of the number of times he has accessed his files on Cloud. These profiles maintain the count of numbers that the file has accessed. If there is any deviation in the user behavior profile already stored in the database, then the attack will be detected.

It is a technique used to find how much a user accessed their information in the web and also used in the commercial sites to detect the fraudulent and track the unusual behavior of a user. Building such a model in fog systems has been really effective since a normal means of access in a cloud service has been continuously checked to identify the any abnormal behavior access to a users' information. This process might include volumetric information on how documents were treated.

To know the victim's search behavior when using their own system which complicatestheir task to mimic the user.The cloud security for implementing additionalfeatures for security expected for profiling the behavior ofusers. When the cloud exhibits the user information thetechnique for profiling the user applied to this model ishelpful in accessing the information provided by thecloud. The behavior for normal user checks thedetermination of abnormal access of normal user. Thisuser information secured by the method for behaviorbased on fault detection

application technologies. Theseprofiles naturally increase the volume of information withthe number of documents which read typically and readoften. The specified features for simple user who coulddetect the abnormality for cloud access where the datatransfer includes the scope for data.

E. Decoy Technology:

The file system is mounted with traps which are uploaded on the system by the CSP. These traps include documents such as credit card details, tax returns, bank statements.These documents are placed in very egregious places. The attacker who is not influenced with the system and who has bad intent may likely to click on these false documents. They may believe that he has Ex-Investigated important information, although they have not. When a decoy document is downloaded an alert will be generated. Through this the system can be notified of an illegal activity.

This technology is integrated with user behavior profiling. When an illegal access is determined and later verified by various methods, such as security question, a disinformation attack may be started. In this attack, the attacker will be given false information and the information they received was believed to be true. This will secure the actual data for the user.

Until now the major challenge in cloud computing is providing desired security over confidential information and its level of assurance to people. Especially problem which concern in securing user data such that no other user can gain access. Whenever a user connects to the internet then the storage of files, documents and media in remote places takes place based on different cloud services and different proposals exists for that. In order to secure the data in cloud, there has been many approaches like standard encryption methods, standard access to controls were made. But all were failed from time to time for various reasons like lack of security procedures, error codes, insider attacks, wrong implementations, failed to envision on creative and effective attacks and misconfigured services. Although providing a trustworthy cloud computing environment is major objective, it's really tough to prevent such attacks in real time, so we can limit the damage of stolen data by decreasing the value of that information to the attacker through preventive disinformation attack Using decoy information as a database for validating the alerts raised by monitoring system carried out by sensors and generating the decoys during that time might improve the efficiency and accuracy of the security in network systems.
There are many documents for generating the decoyinformation which has many honey pot files fordemanding the detection of unauthorized access. Thisinformation to be accessed have extracted informationserves the decoy for confusing and rebating adverseeffect which is not involved in it. Integration of suchtechnology helps in profiling behavior of the userinformation in the cloud service. Cloud service whendeployed with abnormal access towards the noticedinformation returned and delivered in completeappearance of normal user which has legitimateinformation.

The section I explains the Introduction of Cloud computing and techniques used for its security. Section II presents the literature review of existing systems and Section III present proposed system implementation details Section IV presents experimental analysis, results and discussion of proposed system. Section V concludes our proposed system. While at the end list of references paper are presented.

III. LITERATURE REVIEW

Coull et al. in [1] presented a method that is significantly differentiate from other intrusion detection technologies. The method is known as semi-global alignment and is a modification of the

Smith-Waterman local alignment algorithm.The authors enhanced the method and presented a sequence alignmentmethod using a binary scoring and a signature updating scheme to deal withconcept drift [2].

Oka et al. [5][6] had the intuition that the dynamic behavior of a user arising in a sequence can be captured by correlating not only connected events,but also events that are not adjacent to each other while appearing within acertain distance (non-connected events). Based on that intuition they have developedthe layered networks approach depends on the Eigen Co-occurrence Matrix.

Naive Bayes classifier applied by Maxion and Townsend [3] , which has beenwidely utilized in text classification tasks, and they provided a thorough and detailed investigation of classification errors [4] highlighting why some masqueradevictims are more vulnerable than others, and why some masqueraders are more successful than others. Authors also designed a new experiment,which they called the "1v49" experiment, in order to conduct this error analysis.

In [7] Yung proposed another approach term as a self-consistent naive Bayes classifier and was applied on the same data set. Wang and Stolfo utilized a naive Bayes classifier and a Support Vector Machine (SVM) to detect masqueraders [8]. Their experiments confirmed, that for masquerade detection, one-class training is as effective as two class training.

A major goal of hackers is to have control over as systemby which hackers will have the ability to monitor, intercept,and modify system events and activities. Control of a systemis determined by which side occupies the lower layers in the software stack, [9]. Where lower layers control upper layersbecause lower layers

In Cloud, on-premise application deployment model, thesensitive data of each enterprise continues to reside within theenterprise boundary and is subject to its physical, logical andpersonnel security and access control policies. However, insome Cloud model such as public Cloud, the enterprise data isstored outside the enterprise boundary, by the CSP [10].

Author in this similar to [11], assume that the system is composed of the following parties: the Data Owner, many Data Consumers, many Cloud Servers, and a Third Party Auditor if necessary. To access data files shared by the data owner, Data Consumers, or users for brevity, download data files of their interest from Cloud Servers and then decrypt.

We introduce a model for provable data possession (PDP)[12] that allows a client that has storeddata at an untrusted server to verify that the server possesses the original data without retrievingit. The model generates probabilistic proofs of possession by sampling random sets of blocksfrom the server, which drastically reduces I/O costs. The client maintains a constant amountof metadata to verify the proof.A hybrid cloud environment in whichconsisting of multiple internal or externalproviders will be typical for many enterprises.There are many types of security issues in cloudcomputing. Due to these issues, attacks are possible in cloud.

Chen Danwei[13],discussed mainly cloud service security. Cloud service isdepending on Web Services and it will face all kinds ofsecurity issues including what Web Services face.The development of cloud service closely relatesto its security therefore the research of cloudservice security is a very important theme.

Thispaper explain cloud computing and cloud servicefirstly and then gives cloud services access controlmodel based on UCON and negotiationtechnologies and also designs the negotiationmodule.

Shantanu Pa[14], focuses on thedevelopment of a more secure cloud environmentto detect the trust of the service requestingauthorities by using a novel VM (VirtualMachine) monitoring system. The frameworkcan be utilized to provide security ininfrastructure, network as well as data storagein a heterogeneous cloud infrastructure. Theproposed framework tries to maintain thedomain reputation as long as possible bydiscarding malicious users from the domainreducing the CSP's workload. It also increasessome workload of domains and this framework fails to prevent malicious activitywithout CSP's information.

Thecloud hook [15] formation provides a useful analogy for cloud computing, in which the most acute obstacles with outsourced services (i.e., the cloud hook) are security and privacy issues. Here author identifies key issues, which are believed to have long-term significance in cloud computing security and privacy, based on documented problems and exhibited weaknesses.

Embedding the decoy files by monitoring the accessfor signaling the activity of attacks on system can carrymessage for authentication code which is hidden in theheader of documents. The computation over contents offile use the unique key for each user with decoydocument loaded in memory for verifying the decoy document [16]. Depends on the contents of document thecomparison for deemed alert for decoy technique will bedone.

To monitor data accesswhich suspects and verify attacks send large amounts of decoy information [17]. They also can misuse real user data whichevidences the level of data security provided in cloud security. In this model we propose approach for securing data using fogcomputing. This technique used for launching disinformation attacks against malicious insiders which prevents them fromdifferentiating the sensitive data provided from the fake useless data.

This process alleviates the malicious insider from thecloud storage area who uses offensive technique for attacking.

of Amazon's IaaS offerings. In the software as a service (SaaS) service model, the provider installs and operates application software on a cloud infrastructure. Clients may then access the software using a service-specific client software or a generic web browser interface. As with PaaS, SaaS providers are often consumers of IaaS. An example of this would be Dropbox. Dropbox allows clients to store their data and access it from any location via either the Dropbox website or the software one can install on their personal machine. Note that Dropbox has its software running overtop Amazon's S3 service for mass data storage [20]. Netflix is also a company that both provides and consumes cloud computing services. Netflix allows consumers to access movies and TV shows from any location via their website or installed application. While providing this service, Netflix layers their software and functionality atop Amazon Web Services [19].

IV. SYSTEM ARCHITECTURE

Here in Fig.1 show the system architecture.

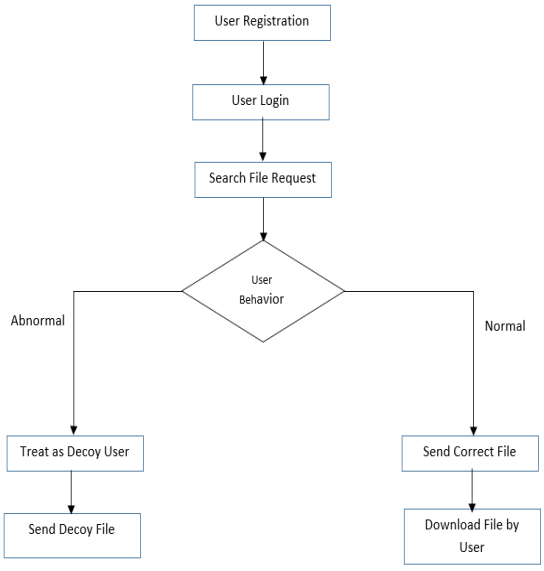

Fig 1. System Architecture

V. RESULT AND DISCUSSIONS

A. Experimental Setup

All the experimental cases are implemented in Java in congestion with Netbeans tools, algorithms and strategies, and the competing classification approach along with various feature extraction technique, and run in environment with System having configuration of Intel Core i5-6200U, 2.30 GHz Windows 10 (64 bit) machine with 8GB of RAM.

VI. CONCLUSION

Monitoring the activity of the cloud user in Infrastructure as a service (IaaS) cloud environments is an important work. Because lots of data shared over cloud. So proposed numerous techniques for maintaining security of cloud called cryptographic technique encryption decryption. But encryption fails to prevent data from attacker in case encryption key is lost. We propose new technique for detecting the intruder or attacker in the cloud and overcome problem present is earlier techniques. But there are no specific profiling strategies for cloud storage area protection and there are no clear differentiation strategies for detecting the attacker's activity. Hence, proposing an efficient strategy for quickly adopting the user's behavior by using decoy technology and user behavior profiling. These recommendations should guide the deployment of decoy documents for effective masquerade detection by finding user behavior and avoiding misuse of information.

VII. REFERENCES

[1]. S. E. Coull, J. Branch, B. Szymanski, and E. Breimer. Intrusion detection: A bioinformatics approach. In Proceedings of the 19th Annual Computer Security Applications Conference, pages 24{33, 2001.

[2]. S. E. Coull and B. K. Szymanski. Sequence alignment for masquerade detection. Computational Statistics and Data Analysis, 52(8):4116{4131, 2008.

[3]. 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.

[4]. R. A. Maxion and T. N. Townsend. Masquerade detection augmented with error analysis. IEEE Transactions on Reliability, 53(1):124{147, 2004.

[5]. M. Oka, Y. Oyama, H. Abe, and K. Kato. Anomaly detection using layered networks based on eigen co-occurrence matrix. In Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection, 2004.

[6]. M. Oka, Y. Oyama, and K. Kato. Eigen co-occurrence matrix method for masquerade detection.

[7]. K. H. Yung. Using self-consistent naive bayes to detect masqueraders. In PAKDD'08: Proceedings of the 8th Pacific-Asia Conference on Knowledge Discovery and Data Mining, pages 329{340, 2004.

[8]. K. Wang and S. J. Stolfo. One-class training for masquerade detection. In Proceedings of the 3rd IEEE Workshop on Data Mining for Computer Security, 2003.

[9]. Anthony Bisong and M. Rahman, "An Overview of the Security Concerns In Enterprise Cloud Computing," International Journal of Network Security & Its Applications, Vol. 3, pp. 30-45, 2011.

[10]. Open Security Architecture Available: http://www.opensecurityarchitecture.org.

[11]. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proc. of ESORICS '09, 2009.

[12]. Provable Data Possession at Untrusted Stores∗Giuseppe Ateniese† Randal Burns† Reza

Curtmola†Joseph Herring† Lea Kissner‡ Zachary Peterson† Dawn Son

[13]. Chen Danwei, Huang Xiuli, and RenXunyi, “Access Control of Cloud Service Based on UCON”, 2011, Nanjing University of posts & Telecommunications

[14]. Shantanu Pal, SunirmalKhatua “A New Trusted and Collaborative Agent Based Approach for Ensuring Cloud Security”, 2011, IEEE

[15]. Cloud Hooks: Security and Privacy Issues in Cloud Computing

[16]. B. M. Bowen and S. Hershkop, “Decoy Document Distributor: http://sneakers.cs.columbia.edu/ids/fog/,” 2009. Online. Available: http://sneakers.cs.columbia.edu/ids/FOG/

[17]. Alleviating Malicious Insider in Cloud Through Offensive Decoy Technology

[18]. Dropbox, “Dropbox help - where does Dropbox store everyone’s data? ” https://www.dropbox.com/ help/7/en, accessed on March 15, 2013.

[19]. J. Ciancutti, “Four Reasons We Choose Amazon’s Cloud as Our Computing Platform,” http://techblog.netflix.com/2010/12/four-reasons-we-choose-amazons-cloud-as.html, accessed on March 15, 2013.

[20]. G.Rajesh Babu, Ananth Kumar ,”Security In Inter Cloud Data Transfer” International Journal of Innovative Research in Computer Science & Technology (IJIRCST) ISSN: 2347-5552, Volume-2, Issue-5, September-2014.

Cite this article as :

Sonam Satyanarayan Tiwari, Prof. Roshani Talmale, "A Review on User Behavior Profiling and Decoy Technology in Cloud Computing", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), ISSN : 2456-3307, Volume 6 Issue 2, pp. 205-212, March-April 2019. Journal URL : http://ijsrset.com/IJSRSET196235