IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 38-44

Designing Security Implementation in Cloud Computing Depend On User Behavior and Decoy Technology

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] *Dept. of Computer Science and Engineering Tulsiramji Gaikwad-Patil College of Engineering and Technology Nagpur, Maharashtra, India*

Abstract: *Recently information technology growing fast to provide users with various services like data access, upload data and download it from anywhere using internet 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 number of industry. Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over theweb. Cloud computing efficiently modifies the way we utilize computers and guarantees access and storage of our private data and business information. These new computing and communication models face new data security challenges. To keep sensitive userdata confidential from untrusted servers, traditional methods usually apply cryptographic methods like encryption by sharing data decryption keys only to genuine 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 remove these issues in the cloud by utilizing decoy technology and user behavior profiling. The users that are using the cloud are trapped and their access patterns are recorded. Every User has a unique profile which is monitored and updated. Here monitor data access by the users in the cloud and find abnormal data entry patterns. When unauthorized user try to access or is detected we begin the wrong attack by returning the bulk of the information to the attacker. This protects users' real data from being misused.*

Index Terms: *Cloud Computing, Encryption, Security, Decoy Technology, User Profiling Behavior.*

I. Introduction

Cloud computing model is flexible for information access and computer resources from anywhere that connection of network is available. Cloud computing gives a resources pool which was distributed among users consist of networks, data storage space, specialized corporate, user applications and computer processing power. It 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 service provider interaction. The CC modelhas three service models and four deploymentmodels. The three service models also known SPI model. A number of computing resources provided over the web. Aninternet based computing is an environment where you pay only for resources that you useknown as 'pay as you go'. Cloud have three party'suser, Cloud service provider (CSP), Cloud provider (CP).CSPare Amazon IBM, Google's Application, Microsoft Azure etc., provide theusers a services to develop applications in cloud environment and to access them from anywhere. Cloud data are stored and accessed on aremote server with the help of services provided by CSP.

A. Services of Cloud

i. Software as a Service (SaaS):

SaaS assures that completeapplications are hosted on the web and users utilize them. Users need not to be install and run the application on the localcomputer, thus it the customer's burden for software maintenance.

ii. Platform as a Service (PaaS):

In PaaS model the CP provides a platform touse.Services provided by this model utilizes 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. 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 isVirtualization. Usually platform-independent; infrastructurecosts are shared and thus reduced; service level agreements(SLAs); pay by usage that is pay as u go model; self-scaling. Avoid capital expenditureon hardware and human resources; reduced ROI risk; lowbarriers to entry; streamlined and automated scaling butdisadvantages are Business efficiency and productivity largely depends on the vendor's capabilities; potentially greater longtermcost; centralization requires new/different securitymeasures. 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.

B. Security of 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 type of failure occurs, it is not clear who is the responsible party. A failure can occur for numerous reasons: because of hardware, which is in the IaaS layer of the cloud;becauseof virus in software, which is in the SaaS layer of the cloud; 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 user's application by adding bogus data. Whatever the reason, a failure can outcome 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.

C. Parties of cloud computing

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-dependent Chrome book.
*ii) Application:*A cloud application is software provided as a service. It have: 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 called as 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 stated as IaaS deliver computer infrastructure typically a platform virtualization environment as a service, along with raw storage and networking.
*v) Server:*The Layers consist both hardware and software; these are on the server. Products that are specifically implemented 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 CC which is utilized to detect when and how frequently the user access his data in the cloud. The way to access cloud user information is predictable. This type behavior of the user is continuously checked for abnormal activity. Each user has its unique profile consist of the number of times he has accessed his files on cloud. These profiles maintain the count of that file has accessed. If there is any change in the user behavior profile already stored in the database, then the attack will be identified.And we called it as user behavior profiling.

It is a technique utilized to detect how much a user accessed their information from the web and also utilized in the commercial sites to predict the theft and track the abnormal behavior of a user. Building such a

model in cloud has been really efficientdue to a normal means of access in a cloud service has been continuously checked to detect the any unusual behavior access to a users' data.

To understand the victim's search behavior when utilizing their own system which complicatestheir task to imitate 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 isneedful in accessing the information provided by thecloud.

The behavior for ordinary client checks the assurance of strange access of typical client. This client data verified by the technique for conduct dependent on fault recognition application technologies. These profiles normally increment the volume of data with the quantity of records which read ordinarily and read frequently. The predetermined features for straightforward client who could identify the irregularity for cloud get to where the information exchange incorporates the degree for information.

E. Decoy Technology:

The file system is mounted with devices which are transferred on the system by the CSP. These devices incorporate archives, for example, credit card details, tax returns, bank statements. These reports are set in offensive spots. The assailant who isn't impacted with the system and who has terrible plan may prone to tap on these bogus archives. They may trust that he has Ex-Investigated vital data, in spite of the fact that they do not have. At the point when a decoy document is downloaded an alarm will be produced. Through this the system can be advised of an unlawful action.This technology is incorporated with user behavior profiling. At the point when an unlawful access is resolved and later checked by different strategies, for example, security question, a disinformation assault might be begun. In this assault, the assailant will be given false data and the data they got was accepted to be valid. This will verify the genuine information for the client. Up to this point the real test in CC is giving desired security over secret data and its dimension of affirmation to individuals.Particularly issue which worry in verifying client information with the end goal that no other client can get access. At whatever point a client associates with the web then the capacity of files, documents and media in remote places happens dependent on various cloud services and diverse recommendations exists for that. So as to secure the information in cloud, there has been numerous methodologies like standard encryption techniques, 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. In spite of the fact that giving a reliable CC environment is real goal, it's extremely hard to avoid such assaults progressively, so we can restrain the harm of stolen information by diminishing the estimation of that data to the assailant through preventive disinformation assault Using decoy data as a database for approving the cautions raised by checking framework completed by sensors and producing the decoys amid that time may improve the effectiveness and precision of the security in network systems.

There are various documents for producing 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. Incorporationof suchtechnology helps in profiling behavior of the userinformation in the cloud service. Cloud service whendeployed with unusual access towards the noticedinformation returned and delivered in completeappearance of normal user which has legalinformation.

For each newly generated folder or a document, corresponding decoy file will be prolonged. The directory and file structure are similar to both the decoy file system and the original file system. The information contained in the decoy document is not original.

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.

II. Literature Review

Coull et al. in [1] introduced a strategy that is altogether separate from other interruption recognition technologies. The technique is known as semi-global alignment and is a change of the Smith-Waterman nearby arrangement algorithm. The authors improved the strategy and exhibited a sequence alignmentmethod utilizing a binary scoring and a signature updating scheme to manage idea drift [2].

Oka et al. [5][6] had the instinct that the dynamic correlating of a client emerging in a sequence can be caught by corresponding associated occasions, yet in addition events that are not nearby one another while

showing up inside a specific distance (non-associated events). In view of that instinct they have built up the layered systems approach relies upon the Eigen Co-occurrence Matrix.

Naive Bayes classifier applied by Maxion and Townsend [3] , which has been broadly used in text characterization tasks, and they gave a careful and definite examination of classification blunders [4] featuring why some disguise unfortunate casualties are more helpless than others, and why a few impostors are more successful than others. Authorslikewise planned another experiment, which they called the "1v49" experiment, so as to direct this error examination.

In [7] Yung proposed another methodology term as a self-predictable naive Bayes classifier and was connected on similar informational index. Wang and Stolfo used a naive Bayes classifier and a Support Vector Machine (SVM) to recognize impostors [8]. Their experiments affirmed, that for disguise identification, one-class preparing is as powerful as two class preparing.

A noteworthy objective of hackers is to have authority over as system by which programmers will be able to screen, catch, and change system events and exercises. Control of a system is dictated by which side possesses the lower layers in the product stack, [9]. Where lower layers control upper layers since lower layers

In Cloud, on-premise application deployment model, the critical information of every undertaking keeps on living inside the enterprise limit and is liable to its physical, sensible and work force security and access control approaches. In any case, in some Cloud model, for example, open Cloud, the endeavor information is put away outside the enterprise limit, by the CSP [10].

Author in this like [11], accept that the system is composed of the accompanying gatherings: the Data Owner, numerous Data Consumers, many Cloud Servers, and a Third Party Auditor if vital. To get to information documents shared by the information proprietor, Data Consumers, or clients for quickness, download information records of their enthusiasm from Cloud Servers and afterward decrypt.

We introduce a model for provable data possession (PDP)[12] that allows a client that has stored data at an untrusted server to verify that the server possesses the original data without retrieving it. The model creates probabilistic proofs of possession by sampling random arrangements of blocks from the server, which drastically diminishes I/O costs. The client maintains a constant amount of metadata to verify the proof. A hybrid cloud environment in which consisting of multiple internal or outer providers will be typical for some enterprises. There are numerous kinds of security issues in cloud computing. Because of these issues, assaults are possible in cloud.

Chen Danwei [13], discussed mainly cloud service security. Cloud service is depending on Web Services and it will confront a wide range of security issues including what Web Services face. The development of cloud service closely identifies with its security therefore the examination of cloud service security is an important topic.

This paper explain cloud computing and cloud service firstly and afterward gives cloud services get to control model dependent on UCON and negotiation technologies and furthermore designs the negotiation module.

Shantanu Pa [14], focuses on the development of a more secure cloud environment to identify the trust of the service requesting authorities by using a novel VM (Virtual Machine) monitoring system. The framework can be utilized to provide security in infrastructure, network just as data storage in a heterogeneous cloud infrastructure. The proposed framework tries to maintain the domain reputation to the extent that this would be possible by discarding malicious clients from the domain reducing the CSP's workload. It also increases some workload of domains and this framework fails to forestall malicious activity without CSP's information.

The cloud snare [15] development gives a helpful relationship to cloud computing, in which the most intense snags with redistributed administrations (i.e., the cloud hook) are security and protection issues. Here author recognizes key issues, which are accepted to have long haul hugeness in cloud computing security and protection, in light of documented issues and displayed shortcomings.

Installing the decoy files by checking the entrance for flagging the action of assaults on system can convey message for verification code which is covered up in the header of archives. The calculation over substance of file utilize 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 screen information, get to which suspects and check assaults send a lot of decoy data [17]. They additionally can abuse genuine client information which confirms the dimension of information security gave in cloud security. In this model we propose approach for verifying information utilizing haze computing. This strategy utilized for propelling disinformation assaults against vindictive insiders which keeps them from separating the touchy information gave from the phony pointless information.

This procedure reduces the noxious insider from the cloud storage zone who utilizes hostile system for assaulting of Amazon's IaaS contributions. In the SaaS service model, the provider introduces and works

application software on a cloud infrastructure. Clients may then access the product utilizing an administration explicit customer software or a conventional internet browser interface. As with PaaS, SaaS providers are frequently purchasers of IaaS. A case of this would be Dropbox. Dropbox enables customers to store their information and access it from any area by means of either the Dropbox site or the product one can introduce on their own machine. Note that Dropbox has its product running overtop Amazon's S3 administration for mass information stockpiling [18]. Netflix is likewise an organization that both gives and devours cloud computing administrations. Netflix enables buyers to get to films and TV appears from any area through their site or introduced application. While giving this administration, Netflix layers their product and usefulness on Amazon Web Services [19].

III. System Architecture

D. System Architecture

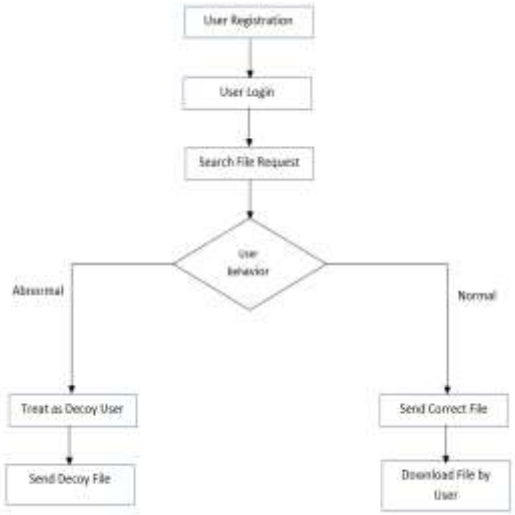

Fig 1. System Architecture

Here in Fig.1 show the system architecture. User first register and then login with credential. Then he searches file request based on that user behavior estimated called as user profiling behavior. If it is normal, then it is genuine user hence send correct file to that user then user download that file. If user behavior is abnormal then that user is fraudulent or malicious user treat that user as decoy user then decoy file is send to that decoy user, he assumes that file received is original file but is not the case he receives the decoy file.

E. Algorithm

1) Algorithm For detecting User Behavior

Output: Detect the behavior of the user Ui

BEHAVIOR 1 ILLEGAL;
BEHAVIOR 2 LEGAL;
Ui → Current User
Log_Details(Uim) → Include all activity of User(Ui)
while TRUE do
if Anonymous_Activity(Ai)
then
++Log_details(Uim)
else
continue;
end
if Log_details (Uim > THRESOLD th) then
BEHAVIOR(Ui) = 1
else
BEHAVIOR(Ui) = 2
end
end

IV. Result And Discussions

F. Experimental Setup

All the experimental cases are implemented in Java in congestion with Eclipse tools, algorithms and strategies, and the competing user behavior approach along with data encryption 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.

G. Result

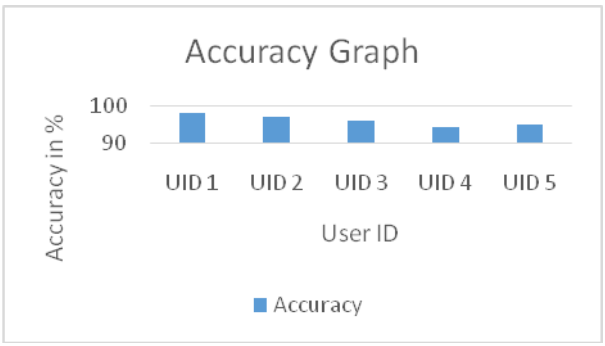

Figure 2. Accuracy Graph

Figure 2 present accuracy graph. In our work we test the system with the help of 5 number of users. Each 5 number of user try to login into our system 20 number of times. The simulation result shown in graph which clearly mention, the number of times we able to detect the behavior of the user correctly. In Figure 2 x-axis show user id while y-axis shows accuracy in %. For accuracy calculation following formula is used.

Accuracy = CCI / TNI

Where,
Correctly Classified Instance = CCI
Total Number of Instance = TNI (20)

V. Conclusion

Monitoring the activity of the cloud user in Infrastructure as a service (IaaS) cloud environments is a vital task. Hencehugeinformation shared over cloud. So proposed various techniques for maintaining security of cloud known as cryptographic technique, encryption and decryption. But encryption fails to prevent data from intruderwhile encryption key is lost. We propose new technique for finding the attacker in the cloud and diminishissuesexisted in earlier techniques. But there are no specific profiling strategies for cloud storage space protection and there are no clear categorization strategies for finding the intruder activity. Hence, proposing an effective strategy for quickly adopting the user's behavior by utilizingdecoy technology and user behavior profiling. These recommendations should guide the insertion of decoy documents for effective intruder detection by recognizing user behavior and avoiding misuse of information. Decoy document contains irrelevant data but decoy user or fraudulent think it as an original file so attacker don't get access to file.

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 Ren Xunyi, "Access Control of Cloud Service Based on UCON", 2011, Nanjing University of posts & Telecommunications

[14].] Shantanu Pal, Sunirmal Khatua "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.