Insider Threat Mitigation in Cloud Computing

Kunal Kumar Mandal
National Institute of Technology
Department of Computer Applications
Durgapur, India

Debayan Chatterjee
National Institute of Technology
Department of Computer Applications
Durgapur, India

ABSTRACT
Insider threat is one of the most critical security threats for any Industry, even it is the most eldest strategy to fall an empire down, very common in diplomacy according to the human history. In the cloud computing ecosystem there are several problems that is harder than the normal (not could) scenarios. If the insider threats are the most dangerous threat even in the non-cloud platform then it must has multi-dimensional attack vectors in cloud computing. Many researches have been done and are being carried out in the field of cyber security for malicious insider attacks. In the provider end of the service, the insider who can harm the system most is the System administrator because he has the highest access control and other privileges. Sometimes when the user demands some resources and the provider is running out of that kind of resource then, they outsource the resource from the third party or cloud broker. The resources are like server, storage and device or public/private cloud. In this paper we propose a technical solution and some policies for the cloud provider to mitigate the insider attack due to the rogue administrator. We also discuss about the possibility of insider attack in outsourcing issue of cloud computing and provide some policies as solution for that problem.

General Terms
Malicious insider, Insider Threat, Cloud computing security, Cloud outsourcing.

Keywords
Malicious insider, Insider Threat, Cloud computing security, Cloud outsourcing.

1. INTRODUCTION
Basic nature of insider threats will remain unchanged in a cloud environment. In cyber security research insider threat is a devious problem so in cloud computing. Although in cloud ecosystem users/customers do not concern about the location and management of their data rather they more concern about the security (Confidentiality, Integrity and Authenticity) of the data kept in the cloud. When a customer signs a Service level agreement then they fully trust the provider and it's a liability of the provider to meet the trust. When an insider attack is committed then there must be some human being involved to the crime, now the challenges are to find the human interactions in the almost automated system like cloud services. Partnering with the USSS (United State Secret Service), CERT (Computer Emergency Response Team) [1] has been conducting the *Insider Threat Study*, gathering extensive insider threat data from more than 700 case files of crimes involving most of the nation's critical infrastructure sectors. 'Attack surface' is that point where people may breach the security in the data/service lifecycle.
Our work is to understand the gravity of the problems, to scheme out the possible ways to minimize attack in a cloud based system. We have tried to find out researches regarding the cloud insider specific threats, pointed out the provided solutions and models to prevent the insider attacks. We are infested in the cloud based scenarios for the proof of concept and at last proposed ideas and policies to thwart the insider attack from the cloud provider point of view.

2. RELATED WORKS IN CLOUD INSIDER THREATS
The paper [2] is a helpful for the malicious insider attacks in the cloud computing environment. They re-define the insiders, malicious insiders, attacks in the context of cloud computing and provide real examples for highlighting the issue of the malicious insider. They addresses a specific problem named as APT (Advanced Persistent Threat), they define the problem like "*APT is of particular concern. If the attacker can access the host OS or the hypervisor, they could propagate across all of the virtual machines on that server and possibly move on to other hypervisors.*" So once the serial access is got for malicious insider, he can reach any VM (Virtual Machine) in the infrastructure. They again show with examples that a malicious insider can install a malicious VM in between the Kernel and the host Os (Operating System) where the host OS operates as a guest OS and provides service for the customers guest operating systems. Now, customers have no idea about how the host OS is installed, as here the attack comes from the providers end and it is almost undetectable as the VMM (Virtual Machine Monitor) is also compromised. Guest OS does not have permission to inspect the host OS activity enforced by the access control of the hypervisor itself. Similarly they have shown various attack surfaces like in Infrastructure as a service "Virtual Machine Cloning". This threat is committed by the malicious insiders from the provider-end with Dom0 permission level. Especially the System administrator, who is an insider, can only be suspected for this type of crime. In their second work [3], they created a set-up like real cloud system used in the IaaS (Infrastructure as a Service) and identify the attack vectors based on their observations which they have found as relevant security problems in the migration of the virtual machines. The virtual machine migration can only be possible by the highly privileged person i.e. The System administrator.

CERT has the most active contribution in the field of insider threat. The paper [4] provides some models and solutions for the malicious insider attacks in the cloud system. They have researched the common vulnerability in cloud based insider attacks and their first concern is "Rogue Administrator". They classify the cloud based system administrators in hierarchy and point out potential vulnerability and/or exploits possible by a rogue administrator. As the protection from the rogue administrator, they suggested the remedy provided in the Cloud Security Alliance [5].

What we can conclude here is that, from the provider's point of view the rogue administrator is the most harmful and dreadful malicious insider for a secure service. Our focus is to mitigate the insider threat by controlling the system administrator's activity and proposing some policies into the provider's organisation for the system administrators. Our work encompasses the points declared in the paper [4] as protecting against rogue administrator and the future research scopes.

3. INSIDER THREATS IN PROVIDER END

According to various researches, insider threat can be done in mainly three perspectives [4]. The first kind of attacks can be done by the rogue administrator as discussed in previous section. In this section we are discussing about the provider end system administrators. Administrators are responsible to manage the service in different layers of cloud. As their role changes the vulnerability in the service and the type of insider attack also be changed. We have found that researchers have proposed a hierarchical role [4] of rogue system administrator. That is shown in Fig. 1.

They can be prevented by the policies and procedures deployed in the organization. CSA (Cloud Security Alliance) has told us about the solutions [5] but the implementation of the procedure is not clearly stated anywhere. To find the sound technical solutions of those policies are an open challenging work. We focus onto that matter and propose a solution with some policies to stop the rogue administrator.

The other two major problems and their solution discussed by them with references by the policies enforced in the organisation and by IDPS on the system. Two models named as Socio-Technical Model and Model Based Prediction [4],[6] also can be applied to hinder the insider attack in cloud computing. The models are still in challenging phase because they are not developed fully.

3.1 Prevention against the Rogue Administrator

Now the proposed policies for the cloud system provider for the rogue system administrator are listed below with reason:

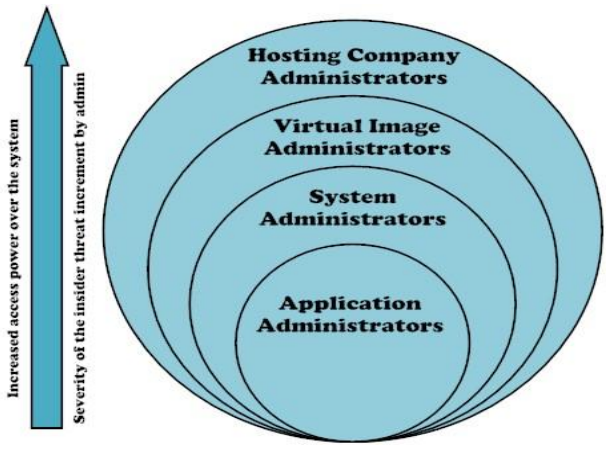

Fig1. Hierarchical view of Rogue Administrators in Cloud Provider & their access privilege, harmfulness

3.1.1 Proposed Policies

a)Group of Administrators must be appointed

Reason: It is an effort to apply Socio-Technical approach. Shared authentication technique may be applied to grant the permission to perform any security critical operation by any system administrator. If everybody/at most some of them conforms the operation by sending their permission, then only the operation can be performed otherwise not. The engineering behind this approach is discussed later in this paper in details.

b) No manual communication possible between co-administrators

Reason: There is a concept in the insider threat known as 'Elucidating the insiders' - means provoking someone to become rogue. Someone like rogue administrator always tries to involve other persons into that crime if and only if that victim is suffering from the same conditions and that rouge admin understands the victim personally well. So, if the rogue admin is sympathetically or by blackmailing got success to establish a connection manually to the other administrator then he can easily get the secret information from targeted personal, what ultimately brings the success for an insider threat.

c)Better to place Administrators geographically isolated

Reason: There is no surety that one administrator meets another eventually or coincidentally somewhere if they are in the same city or town. All the concerns said in the previous point will true if they somehow revels the truth about each other. As for recommendation the administrators should be placed isolated as far as possible, keep unknown about the location of others like cloud. This will never hamper their work because they are connected through the network for their job.

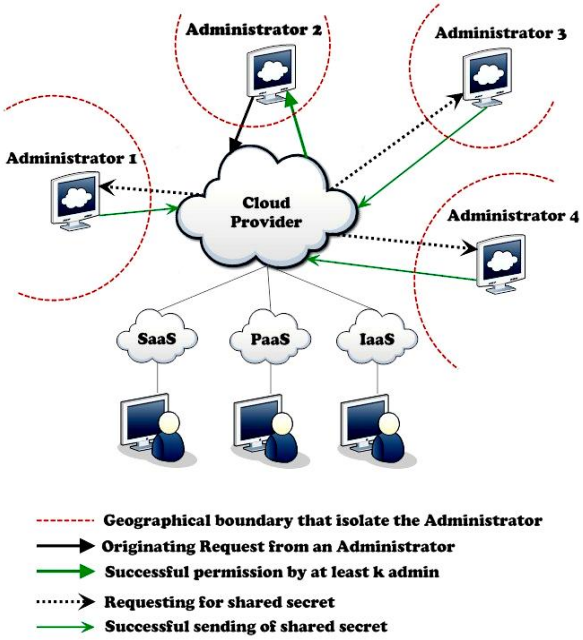

Fig 2. Schematic diagram of the communication among the administrators in the service provider side

d) Agreement not to share said information in the social networks or chat servers

Reason: Assume, administrators are publishing the Company name, job profiles and information about duties in the social network sites. Then rogue administrator may find his pray by

intelligent search in the social sites and that brings a major chance for elucidation.

e) Balanced leave policy among administrators

Reason:
Although it depends on the organisation that among N number of administrators how many would go to the leave at the same time because, in this multiple authentication procedure those requests from one admin will be awaited for the permission of the others. This issue is also addressed in the technical details when we will discuss about the authentication procedure. There is a solution for balancing the leave and that is separation of duties [7].

f) Must apply Insider Threat detection/prevention technique

Reason:
For any organisation, the common policies told by CERT [8] can be applied for prevention of insider threat. In this situation as the cloud provider is also an organisation and if they follow the policies and procedures to protect the data (mainly client data, vm images, confidential data of clients) from stealing the information, "Theft of confidential or proprietary data" – very common attack vector in insider attack, then they are actually minimizing the insider attack in cloud computing. Efforts [9] are already made to catch the malicious insider within the organisation.

g)Log based monitoring system

Reason:
Log must be maintained to store the history of the incident performed by the system administrator especially for the security critical operations. Even the log must not be written /changed by the administrator with the highest permission. The log can be used by the insider threat detection and forensic analysis. It is a challenging work to utilize the log efficiently and timely manner.

3.1.2 *Technical Details for preventing the attack by Rogue Administrator*

As we told before, in this section we elaborate and explain the technical details to manage the multiple administrator authentication system and its effect in the system good and bad. The necessary requirements are stated below to deploy the plan:

a) Requirement

Req. A: Group of Administrator (as said in Policy a).

Req. B: Secured communication channel (just for message passing among the admins) but holding the policy b and c) The chat history also maintained.

Req. C: Admin portal View for the multiple administrators.

b) Procedure

A notification system is built (as per the req. B) such a way that it uses a secured communication channel (like: secure chat server) where one admin writes message/request to all the system administrators (available, maintaining the Policy e.) on that time. If and only if k numbers of administrators are agreed upon with the validity of the operation then only the requesting administrator acknowledges permission to do the job, shown in fig. 2. Here for the provider organization, they must maintain a threshold for the administrator on the leave. In this type of scenario at most (N-k-1) numbers of administrator may be on vacation at the same time.

Where, $1 \leq k \leq N$; N = Total number of participant administrators.

The broadcast message consists of technical reason of the operation in brief. All the system administrators must check real scenario by their portal (as per the req. C). After looking into the fact, the administrator should take the decision as soon as possible. When at least k numbers of valid data is gathered then the permission to do the job will be granted otherwise the job will not be permitted.

In the way for relaxation of the security and increment of the user friendliness or less secured data handling, we propose to tune the value of the 'k' down. Actually the minimal permission support i.e. hardness of the permission grating procedure is dependent on the value of 'k', decreasing the value helps the system to run in the low insider threat detection/prevention mode. However, it creates a situation where the human resources (administrators) are not fully utilized for this very purpose i.e. mitigation of the insider threat.

c) The way of providing permission

There are several schemes to facilitate such kind of scenarios. Most well known way of doing is "Shamir Secret Sharing" [10]. There are two types of secret sharing, one is, N- out-of-N and k-out-of-N secret sharing. Choosing the scheme is totally dependent upon the provider but for any scheme the provider must keep the policy e. in mind for establishing the sharing.

In the secret sharing, a piece of information is divided among the administrators. When requesting administrator asks permission from the k numbers of participating administrator then a window (user interface) for accepting the password/secret information with captcha image (optional) is popped up to the screen of the N participating administrator. After the verification of the request, at least 'k' numbers of person send their secret piece of information which reconstructs the main key to permit the operation for the requesting administrator. Any other advanced technology for secret sharing scheme may be used. Here we propose Shamir's threshold secret sharing as for instance.

Something is very important for the administrator to maintain for this type of authentication:

- The work will be delayed until one among the k is not providing his secret key, which leads to a very common problem in the cloud that is Denial of Service (DOS). So, as quick as possible the administrator has to verify the authenticity of the request by investigating the situation and then provide the secret key.
- If some confusion arises, then ask back to the requesting admin for the reason by the secure communication/chat service. Should not waste time too much.
- The denial of providing secret key is a high indication to an insider threat and it is logged by the system. Unless one is sure that it leads to an insider threat or some vulnerable activity, he should not raise an alarm and delay in the process.

3.1.1 Test Case Scenario

Assume there are four system administrators {A1, A2, A3, A4} in a group responsible for managing particular level of service. They are equally qualified as accordance to the organization for the post of the system admin. Now, it may happens that one (Let, A2) among that group become rogue but to perform a critical operation needs the permission of at least k number of administrators out of N to grant the permission.

Now for the example, A2 the requesting administrator, seeks the permission to do 'VM image copy' – sometimes it is the common job for a system admin to back-up the image of the host system, but it may be a malicious activity. As our assumption A2 is malicious then he tries to do something malicious with the host images. Then the other administrators, at least two among the three (let k = 2) are not agreed with it for some reason which they think as harmful or may be vulnerable to the system. If they find something fishy, they can raise an alert.

They can judge the operation by the portal provided to them by which the can see the provider cloud system on that very instant. Even anyone can ask back to the requesting administrator (A2) for clarification by the secured communication channel.

3.2 Insider Threats in Cloud Outsourcing

Sometimes, provider of the cloud outsources resources [11-13] from cloud broker or the third party cloud for the reasons below:

- If the provider is running out of that kind of resources.
- To save the space and cost. Sometimes the provider borrows the resources from the third party and provides the customer with some higher rate than the charges he gives to the third party – a common business strategy.
- Low maintenance cost – during the time when the customer uses the system then no extra staff is required for the provider to maintain the system, because that system is actually provided and managed by the third party. When the customer releases the system the provider easily return the system back to the third party after backing up the state of the system properly.
- For the security purpose – For some security critical reasons the provider lends the secured system from the trusted, secured cloud service provider/third party. No extra care needs to be taken for this purpose.

All the above cases, there are issues of trust between the cloud service provider and the third party. The service level agreement primarily holds the trust between them.

If some threats are found in the service, the customers sue the service provider and service provider eventually has found that the problem with the borrowed resources and it may be caused by some malicious insider on that third party cloud. Now the service provider falls into serious trouble because they cannot show the customer what the real situation is, moreover customer does not bother about it. The service provider has to take the responsibility over the crime as like as insider threat although it is not committed by the real insider within their company.

In this case the malicious insider is the System Administrator in the third party cloud system which shares the requested resources to the requesting service provider, but this rogue system administrator is totally out of control and monitoring system applied in the organisation of the service provider. This is one of the most challenging works to mitigate this type threat.

3.2.1 Proposed policies for prevention

We propose some policies to prevent this kind of threat. Those are listed below.

a.) Cloud in collaboration or this kind of crowd cloud must sign to an agreement in collaborative level in terms of that their system will remain insider threat free. If some mishap happens, the necessary measures are also declared clearly.

b.) The strict time of compensation for the loss due to the insider threat (if identified) must be clearly said in the SLA.

c.) Insider threat free certificate (if any) provided by the recognised organisation and validity of the certificate with corresponding documents are also attached in the time of agreement. Regular cloud audit report with respect to the insider threat must be disclosed.

d.) Use some technical procedure for mitigating the insider threat in this type of case. Like:

- Before redirecting the resource to the customer, clear the stored data in the system if the resource is capable of storing some data [14].
- After releasing the resource from the customer, the data must be backed up clearly that means no trace of data should remain in the resource more, because, those data may be the critical data of the customer.
- If it is a VM, checks the state of the VM (updated/ configuration/ access control etc.)
- Keep in monitoring those resources by special care because it is being managed by the third party and they may not be always trusted.

4. CONCLUSION AND FUTURE SCOPE

In this paper, we have discussed about the insider threat in the cloud service provider end with both respect, from a rogue administrator within the organisation and cloud outsourcing problems. Pure technical solutions are seldom found in the research of the insider threat. What we can boldly conclude is that, the technical solutions integrated with valid policies are the most appropriate solution in this threat. Here we've tried to address that problem using the both way. The main limitation in our solution is, it takes much time to respond to the customer requests and sometimes it leads to the Denial of service problem. Now the solution is obviously to loosen the security so the user friendliness is getting high, though it fully depends upon the organization. The way is also discussed in the section A.2.b.The another problem is, the solution increases the cost related to the human resource (System administrator). It is also real challenge for the researchers.

There is huge future scope in this area. As we have found the gravity of the problem, we can judge the wide range of attack vectors, unpredictability and surfaces may exist. There are other problems like guest based attack from the client side elucidating by the rouge insider from the organisation, ways of binding trust in the cloud outsourcing, technical solution for the checking of the borrowed resources, finding a trade-off between the cost of the human resource and the security and so many.

5. REFERENCES

[1] Inside Threat, Source: http://cert.org/insider-threat/research/database.cfm, Last Access : September, 2014.

[2] Adrian Duncan, S. Creese, and M. Goldsmith. Insider attacks in cloud computing. In Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on, pages 857–862, 2012.

[3] Adrian Duncan, Sadie Creese, Michael Goldsmith , and Jamie S. Quinton . "Cloud Computing: Insider Attacks on Virtual Machines During Migration," Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on, pages 493 - 500, 2013.

[4] William R Claycomb and Alex Nicoll. Insider threats to cloud computing: Directions for new research challenges. In *Computer Software and Applications Conference (COMPSAC), 2012 IEEE 36th Annual*, pages 387–394. IEEE, 2012.

[5] Cloud Security Alliance, Source: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, Last Access : september,2014.

[6] Kandias M., Mylonas A., Virvilis N., Theoharidou M., and Gritzalis D., "An Insider Threat Prediction Model", In: Proc. of the 7th International Conference on Trust, Privacy, and Security in Digital Business, LNCS-6264, Springer, Spain, 2010, pages 26-37,2010.

[7] Ravi S. Sandhu: Separation of Duties in Computerized Information Systems. DBSec 1990, pages 179-190, 1990.

[8] Common Sense Guide to Mitigating Insider Threats, Source:http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=34017, Last Access : september,2014.

[9] Spitzner L., "Honeypots: Catching the insider threat", in Proc. of the 19th Annual Computer Security Applications Conference, USA, 2003, pages 170-179,2003.

[10] Shamir's Secret Sharing, Source: http://en.wikipedia.org/wiki/Shamir%27s_Secret_Sharing, Last Access : september, 2014.

[11] Cloud Computing Synopsis and Recommendations. csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf

[12] Moving from Outsourcing to the Public Cloud, Source : http://blog.isg-one.com/2014/04/29/moving-from-outsourcing-to-the-public-cloud-prepare-for-more-insourcing/, Last Access: september,2014.

[13] IT Outsourcing Risks and How to Mitigate Them, Source: http://deloitte.wsj.com/cio/2012/07/10/it-outsourcing-4-serious-risks-and-ways-to-mitigate-them , Last Access: september,2014.

[14] Li Chaoling , Chen Yue , and Zhou Yanzhou, "A data assured deletion scheme in cloud storage", China Communications· April 2014, pages 98-110, 2014.