OPEN ACCESS

International
Journal
Of Modern Engineering Research (IJMER)

Remote Access and Dual Authentication for Cloud Storage

Balaiah Gari Venkat Ranga Reddy[1], Kavya.A[2]
[1, 2] (Department of Computer Science and Engineering/VIT-Chennai/ INDIA)

Abstract: *Cloud computing is an emerging technology, which provides services over internet such as software, hardware, network and storage. The key role for cloud computing is virtualization which reduces the total cost and gives reliable, flexible and secured services. However compute service are chosen between the providers located in multiple data centres. One of the major security concerns related to the virtualization and the Storage where the outside attackers can use the files in the storage and the data owners are not capable of knowing attacks. In this paper we proposed a high level authentication for the cloud user and remote monitor controlled of your cloud storage. Here our model provides the dual authentication for the cloud and to get the runtime record of the logs and the secured application controls, the logs are remotely accessed and controlled by the owner of the data.*

Keywords: *Attackers, Authentication, Storage, Cloud*.

I. Introduction

Among the cloud services IaaS (Infrastructure as a service) is highly used in the large enterprises where the physical hardware is virtualized and serves to industrial and personal world. Cloud services are cost saving in real business world, and are successful Instead going to traditional cost in purchasing expensive and generation outdated hardware resources.

In virtualization approach several physical servers are connected by switches. The traffic between the servers from switch can't get detailed flow information this impacts some security information. As cloud is an internet based computing model that gives convenient on demand services like Storage as a service in which many business, company and educational societies are moving their services to cloud to store their data remotely located large data centres. The client can authorized to get his data modify, delete and can access remotely anywhere.As the data stored in large volume of data where the malicious attacks can occur at the VM level or at the hypervisor, if a kernel is compromised with rootkits they can easily access or delete the confidential data.

The Hypervisor layer is above the Hardware resources and resides operating system on the hypervisor, it is advantageous to us it gives the natural privilege where traditional security system is built, and the hypervisor acts as the master level in the access to hardware resources and more security levels can be built in hypervisors this paper gives you the dual authentication and the remote access will give the user end of the logs of his cloud storage.

As the cloud clients are need of having the high level authentication check. In the present generation authentication is done in many ways such as, textual, graphical, bio-metric, 3D password and third party authentication [2].In this paper high level authentication is taken care for the cloud clients by introducing the dual authentication technique which generates/authenticates the password in multiple levels to access the cloud services. In this paper, details of proposed dual authentication technique are presented along with the architecture, activities, algorithms and probability in success of breaking authentication is low.

II. Related Work

Most of the work done on the cloud storage security Dexian Chang and Xiaobo Chu has proposed the Flexible root of trust for the cloud[1] specified the attacker model and implemented the lightweight TSD (Trusted Service Domain), root of trust in the virtualization platform which shows the better security and efficiency. Data security in cloud computing based on Virtualization in this study case different type of virtualizations are given where the attacks in the hypervisor and VM level are to be noted, different security attention are given in transferring the data mainly to another cloud.

Thiyagarajan M, Dinesh Kumar K has given the model for authenticating cloud using the QR codes as in this process they use the captured images, the images are decoded with the encoder function() [7] and the data is sent by SMS to the cloud central server to authenticate the user. QR model describes the whole authentication needs an external personal device and also the server will not compromise if any delay in the provider of the mobile.

Authentication of different methodologies were implemented as of digital signature, 3D authentication as there are all at the entry level authorization. Hypervisor is an superior place in the place of authentication as this with the inspection and interposition here the system states are of CPU registers, BIOS, storage are managed the interface of the Operation system the boot loader of the system is loaded in the bios which interfaces the hypervisors, we can say that hardware is the root nodes of the servers.

III. Problem Statement

In the virtual cloud storage the attackers at the VM level is controlled by the authentication where if the Hypervisor is compromised with any of the boot loader it will erase all the security level and turns firewalls off and other security tools. The attackers like DDoS attack in which layering security across the multivendor networks, client to client attacks where One client has malicious and it can infect to other users of all VM's that relay on the physical hardware on the same hypervisor. Mainly authentication is taken at the application or entry level where the attackers can easily attack the user passwords, but in the hypervisor level we can seal the hardware resources with TPM seal as we can modify the security levels at this state which can increase the security levels of the user data stored in cloud.When the data storage is used by others and attackers the owner will not get to known instead confidential data may be modified or deleted in his virtual storage.

IV. Proposed Model

Authentication:

In the cloud services the users need the authentication to access his services. The user can access the cloud services if his authentication was successful, the basic and used model for security in any services is authentication. Authentication is used in two types i) Cloud service provider gets to check the privilege user not any attackers ii) Cloud provider to confirm the SLA's and allocates the specified resources to the client as of formal procedure. This authentication is verified at the internet based of entity logging to the services.

The authentication of user in this model is dual authentication, we add some security levels into the grub which is the boot loader for every physical machine, TPM will seal storage of the users in which the data of the user will be encrypted with encryption tools and the data in the storage can be accessed until the dual authentication is successes. Due to this the malicious attackers will be prevented, TPM seal will be decrypted and the storage will be accessed and system will be start up at this stage.Here in this cloud virtualization first VM level attacks are the main causes for security of data where the data of a user is accessed, and cloud provider can use the data of the user some provider vulnerabilities like SQL-injection and core site scripting which cause insecure of the data. Secondly Hypervisor level attacks when an attack is on hypervisor this an highly security issue he can take control of the whole data centre, issuing this problems we had the dual authentication in which the hypervisor will have and second level authentication between hardware and Virtual machines or hypervisor which holds TPM seal on the hardware.In this real time analysis the probability of attack will be low the TPM will not compromise until the password you entered is permitted, this will not support any reverse engineers (password generator) in this grub level loader the authentication is not saved in a plain texts.

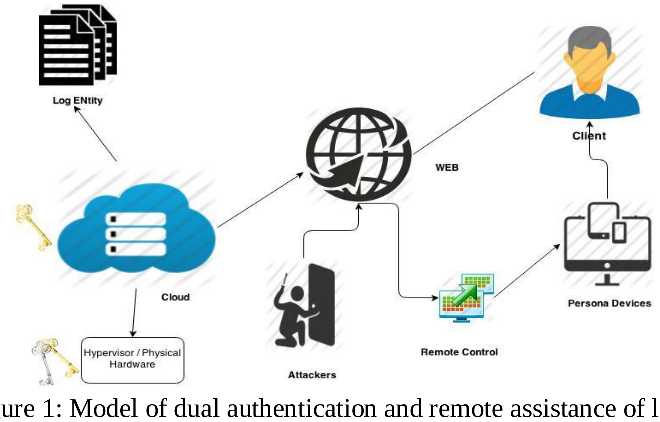

Figure 1: Model of dual authentication and remote assistance of logs

Algorithm for authentication and remote model:

```
Cloud server
{
if (authentication at entry level=succeed)
   {
    Enter the security key for hypervisor level
    if (security=succeed)
```

```
        {
else
          {
return authentication failure;
           }
         }
     Decrypt the TPM seal and give privilege to user;
       {
       MalGen records the logs data;
if (user requests the logs)
proxy is authenticated to remote access;
       }
   }
}
```

Remote Compute of logs in cloud:

In the site entity logs that are compromised with authentication and the data used by the user, time had been recorded in the monitoring tools as MalGen is an open source code owned by Google which gives the logs of the large data sets handled by Hadoop. In this log entity if the entry of the user is compromised by the server then the Flag is set to ‘1’, if it gets incorrect password set to ‘0’.The data format of MalGen is “Event ID|Timestamp|Site ID|Flag|Entity ID”as in our logs the compromised logs areshownas “0079999999600738500244954329305|2014-04-1210:50:41.606070|0445544244954369755|0|0000000000001032397” and the Volatility is the other tool which generates the same logs as they are in the shows GUI of the Hacker when accessed and the directory of access are shown, with this site entity logs the client get over the attack or malicious entry into his cloud.In TheRemote control to the client the server will provide the attestation proxy where the trusted remote access to client, remote login can be accessed by the given proxy he can set to his any personal devices and can be accessed to the logs entity of his cloud storage

V. Conclusion And Future Work

The cloud computing is an emerging technology which reduces the burden of the users and also cost effective resources and used over internet remotely, due to this security issues are also arising where the malicious attackers we can make sure of our data safe by having remote access of our entity logs and we also proposed a model to dual authentication where the user can have his secured cloud.

Dual authentication is where authorised at both the entity of cloud and also the grub level in which takes more time for authentication than the normal authentication we can try to decrease the time for the execution of the whole system in authenticate.

REFERENCES

[1] Hamdi, M., "Security of cloud computing, storage, and networking," Collaboration Technologies and Systems (CTS), 2012 International Conference on , vol., no., pp.1,5, 21-25 May 2012 doi: 10.1109/CTS.2012.6261019

[2] Dinesha, H.A.; Agrawal, V.K., "Multi-level authentication technique for accessing cloud services," Computing, Communication and Applications (ICCCA), 2012 International Conference on , vol., no., pp.1,4, 22-24 Feb. 2012 doi: 10.1109/ICCCA.2012.

[3] Baliga, J.; Ayre, R.W.A.; Hinton, K.; Tucker, RodneyS., "Green Cloud Computing: Balancing Energy in Processing, Storage, and Transport," Proceedings of the IEEE , vol.99, no.1, pp.149,167, Jan. 2011 doi:10.1109/JPROC.2010.2060451

[4] Kumar, A.; Byung Gook Lee; HoonJae Lee; Kumari, A., "Secure storage and access of data in cloud computing," ICT Convergence (ICTC), 2012 International Conference on , vol., no., pp.336,339, 15-17 Oct. 2012 doi: 10.1109/ICTC.2012.6386854

[5] IEEE - The Application of Cloud Computing in Education Informatization, Modern Educational Tech... center Bo Wang, HongYu Xing.

[6] NISTDefinition http://www.au.af.mil/au/awc/awcgate/nist/cloud-def-v15.doc

[7] CA Technologies cloud authentication system http://www.ca.com/us/authentication-system.aspx

[8] X. Suo, Y. Zhu, G. S. Owen, “Graphical passwords: A survey,” in Proc. 21st Annual Computer Security Application. Conf. Dec. 5–9, 2005, pp. 463–472.

[9] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, “Authentication using graphical passwords: Basic results,” in Proc. Human-Comput. Interaction Int., Las Vegas, NV, Jul. 25–27, 2005.

[10] Barsoum, A.; Hasan, A.,"Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems," Parallel and Distributed Systems, IEEE Transactions on , vol.24, no.12,pp.2375,2385,Dec.2013doi:10.1109/TPDS.2012.337.