IOSR Journal of Engineering (IOSRJEN)
e-ISSN: 2250-3021, **p**-ISSN: 2278-8719
Vol. 3, Issue 10 (October. 2013), ||V1|| PP 08-15

Developing trustworthy Cloud with the Help of TTP

Deepti Nikumbh, Manish Potey
[1](PG student(K.J.S.C.E)/ Mumbai University,India)
[2](H.O.D(Computert), K.J.S.C.E/ Mumbai University, India)

Abstract: - Clouds Are Becoming An Interesting Alternative To Dedicated It Infrastructure. However, Cloud Computing Also Carries Certain Degree Of Risk For Both Customers And Cloud Service Providers. There Is A Lack Of Trust In Cloud Which Acts As A Barrier In Widespread Adoption Of Cloud Computing Technology. In Order To Increase Trust In Cloud ,We Need To Make Clouds More Transparent And Accountable For Both Enterprises And End User. Accountability And Transparency Can Be Achieved By Tracking Every Single Activities And Data Transfers Happening Within Cloud Environment.Current Systems Fail To Provide This. Thus, In This Paper We Propose A Framework Which Achieves Accountability By Generating Logs For Every User Activity, Further We Suggest A Kernel Level Encryption Mechanism For Encrypting Log And TTP For Storing And Accessing The Logs.

Keywords: - *Cloud Computing, Logging, Accountability, Trusted Cloud, Detective Mechanism, Files Centric Logging, Cloud Forensics, Trusted Third Party (TTP).*

I. INTRODUCTION

Cloud have attracted a lot of attention in recently. The advantages of cloud are unarguable but cloud computing is like a double edged sword: same properties of cloud which makes it more appealing are responsible for making cloud based crimes, difficult to prevent and investigate. Cloud computing requires companies and individuals to transfer some or all control of computing resources to cloud service providers (CSPs).Such transfers poses concerns since customer releases control over his data and computation. In convectional model i.e. traditional client server model, customers resources, his computations where carried out by servers which were maintained in customer premises, the customer had physical access to these servers and got them managed by the people whom he trusted. In new i.e. cloud computing model customers resources, computation is handled by virtual machines in cloud, management of physical machine is delegated to cloud service provider and customer retains some control on virtual machines which he can manage remotely by network connection [1].Since user's does not have direct control over their resources, trust becomes a critical issue for them. Recent attacks on cloud have strengthened the security concerns. Possible attacks on cloud could be exposure to malicious insider attack or malicious outsiders attack i.e. hacker hacking the system. For example, the servers of the red hat Linux distribution were recently attacked and the intruder managed to introduce vulnerability and even sign some packages of Linux operating system distribution [2].Unauthorized access can also occur by software malfunction at the provider end. Such data breach occurred in Google Docs during march 2009.Another example where data integrity was compromised as a result of provider malfunction is a recent incident with Amazon S3 where user experienced silent data corruption [2].

In a recent 2010 survey by Fujitsu Research Institute on potential cloud customers, it was found that 88% of potential consumers are worried about security of their data, and demanded more awareness on who has access to their data and how the data is maintained on backend physical server [3]. The Cloud Security Alliance, has recognized top threats to cloud computing and is listed below [4]:

[1] Abuse and nefarious use of cloud computing
[2] Insecure application programming interfaces
[3] Malicious insiders
[4] Shared technology vulnerabilities
[5] Data loss or leakages
[6] Account, service and traffic hijacking
[7] Unknown risk profile.

Accountability is a key to address these threats. If CSP achieve accountability and auditability in its cloud architecture five of the above seven threats: 1,2,3,5 and 7 can be reduced[3].

Further, safeguarding of accountability data i.e. logs generated is very crucial in cloud environment since these logs are helpful for carrying out cloud forensics [6]. CSP can collude with other users and can modify the generated logs. For example, he can deleted some logs, reorder some log entries or even add some fake log entries [6]. In this paper we present a framework that achieves accountability and log security. Firstly we present a logging mechanism, this mechanism records all the file-centric access, scp transfers and network activities happening on VM's and data transfer occurring between the VM's and outside world, these log records generated are encrypted using kernel level encryption. Further, encrypted log records are send to TTP i.e. trusted third party for storage and can be access by users through TTP.

II. TRUST IN CLOUD ENVIRONMENT

1.1 Components of Trust in Cloud Computing

Following components are together responsible for achieving trust in cloud environment [5].

1.1.1 Security

Security prevents any unauthorized access to information occurring in cloud. Security, in current cloud environment is achieved to a large extent by sophisticated cryptographic methods.

1.1.2 Privacy

Privacy allows only authorized users to access cloud. Privacy is also achieved to a large extent by different authentication techniques.

1.1.3 Accountability

Accountability record's and track's each individual action happening on service provider's end. In current systems accountability is limited only to generating system logs. More research related to cloud accountability is needed as it is important for enabling auditability and transparency in cloud.

1.1.4 Auditability

Goal of auditability is to trace an action back to the owner. Internal and external audits are both crucial, since it increases trust and transparency in CSP. Following presents a table which shows different mechanisms adopted by each trust components.

TABLE 1.Mechanisms Implemented By Trust Component[5]

Trust Component	**Mechanisms Adopted**
Security	Physical Security, Firewalls, Intrusion Detection System,Strong Encryption Algorithms.
Privacy	Role-based access, Multi-factor authentication, ACL's, VM isolation, Key Rotation, data and VM encryption.
Accountability	System logs which mainly focus on the server status,hardware performance mertices.
Auditability	Internal and External Audits.

For achieving trustworthiness in cloud all the four components i.e. security, privacy, accountability and auditability must be ensured completely.

1.2 Existing Security Control for Trust

In order to increase trust in cloud computing, there are both preventive and detective measures. The mechanisms through which security and privacy are achieved are classified under preventive measures whereas accountability and auditability are classified under detective measures. Many CSP focus on preventive measures eg. Better firewalls, strong encryption algorithms, intrusion detection systems etc and detective measures eg. logging, audit trails, etc are neglected .Due to virtualization and data distribution occurring in current cloud environment there is an urgent need for research in cloud accountability[3].The customers are now more concerned about their data's integrity and confidentiality rather than health and utilization of servers. Accountability being such a crucial component many prominent cloud providers still does not providing full transparency, accountability and data provenance [7] of both the physical and virtual servers utilized [3].Currently, users can at best monitor the virtual hardware performance metrics and the system event logs of the services they use [3].Logs generated mainly focuses on the overall system health indicators i.e. uptimes, processor usage, events, etc. Especially in IAAS environment where users have control on virtual machine, it becomes difficult to implement accountability. Current systems at most can monitor the time stamping

information about when the VM's where started and when the VM's where killed, which are not enough to track user activities.

Log information generated in cloud environment is highly sensitive and user's privacy issue is directly related to it[6]. Current cloud environments does not support cloud forensics, it does not provide a secure way of revealing the logs at the same time maintaining user privacy. Further the investigators has to completely believe that the CSP's are providing the correct information, there is no way to ensure that evidences provided by CSP to investigators are not manipulated. Currently, to collect evidences from cloud, investigators and user's are completely dependent on the CSP. Investigator needs to issue a subpoena to the CSP and then only they can acquire evidence or forensic information of a particular user [6].

1.2.1 Approaches for Accountability

Existing accountability techniques cannot be directly implemented in cloud environment. Cloud's are basically general purpose platforms and it should provide accountability for every services that user wants to run over it. Thus application specific technique like Repeat and Compare[11] is ruled out. The application independent techniques like Peer Review[12] requires that software or services that customer uses should have a deterministic behaviour,but this is difficult to guarantee in existing cloud environment.

Other tools like snort are used for monitoring packet in network. Fig 2 shown the logs generated by snort through BASE. BASE is a php script used to read the logs generated by Snort through a graphical interface. From the figure we can see that snort gives only the network information which alone is not enough to track user activities on cloud.

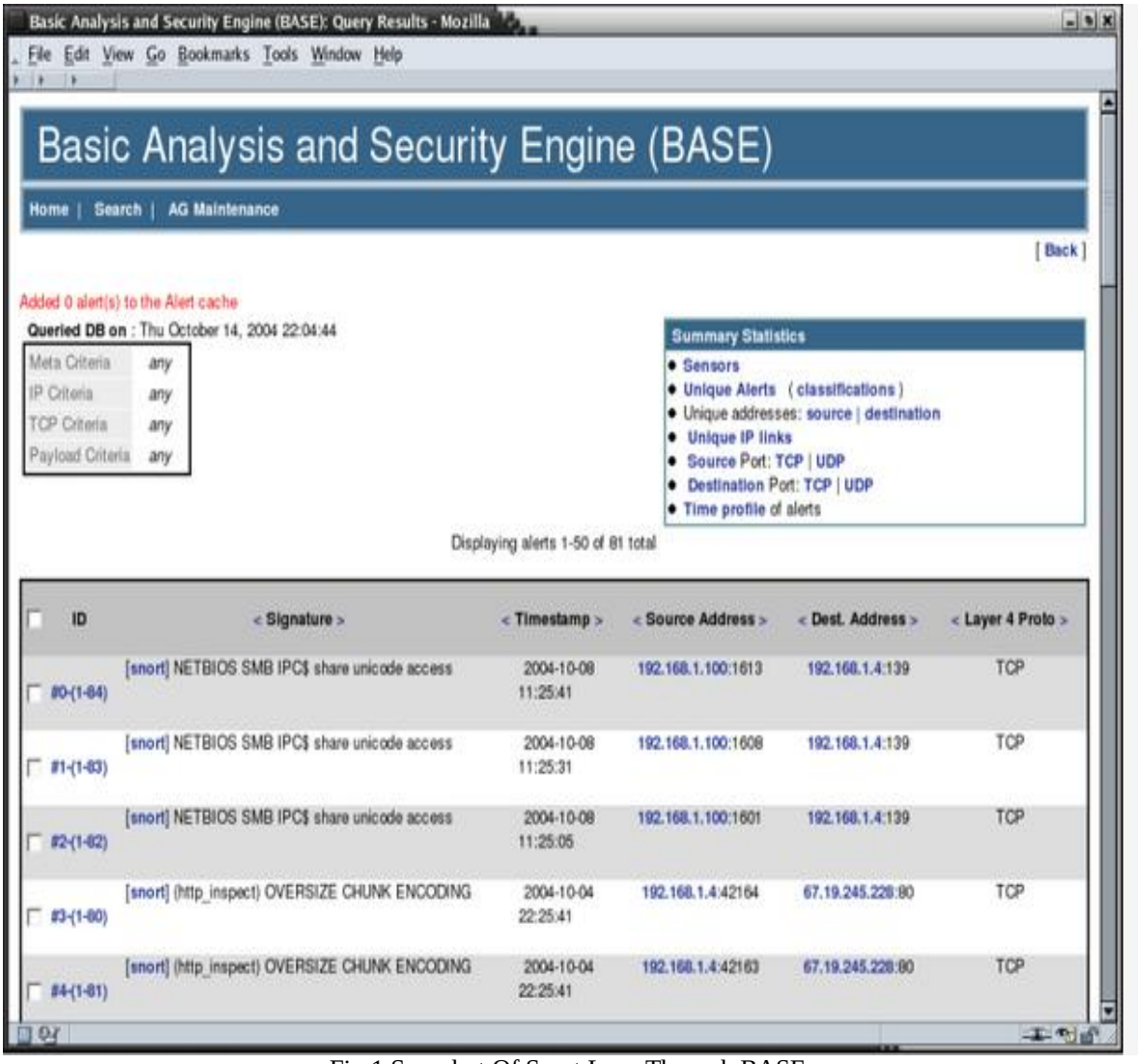

Fig 1:Snapshot Of Snort Logs Through BASE.

With the rise of virtualization technology, tools like HyTrust Appliance[13] are becoming more prominent, HyTrust appliance monitors all the activities done by the administrator and cloud employee on cloud. It maps every action against an access control list and only if the enmployee has the privilidges then only he is allowed to perform it else he is denied, but these tools also does not provide full transparency of the user activities on cloud. Figure 2 gives the snapshot of the quality audit log generated by the Hytrust appliance.

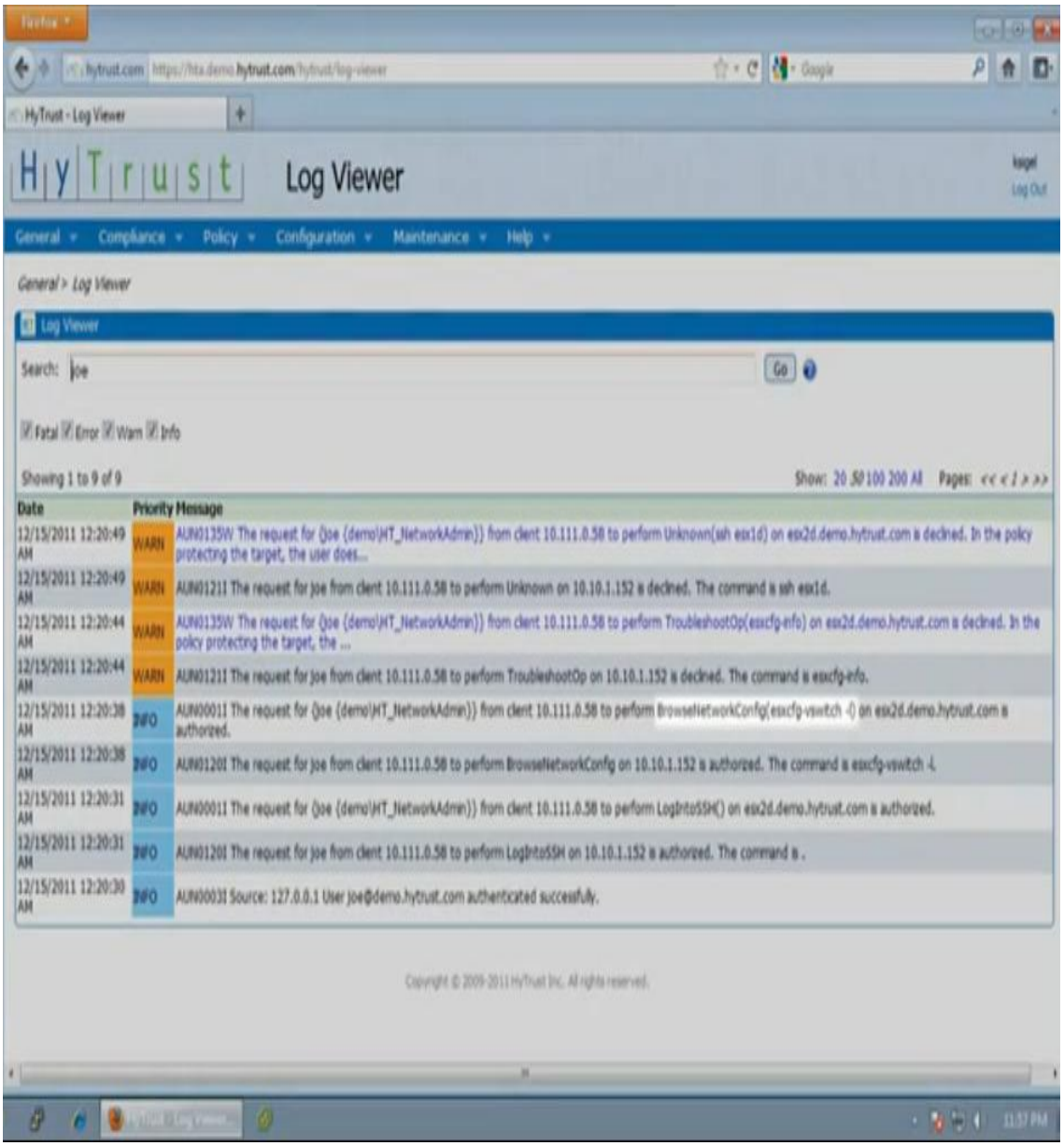

Fig 2:Snapshots of Hytrust Logs[13]

Other tools like CloudKick[14] only focuses on server health and performance. Figure 3 shows a dashboard provided by cloudkick.Cloudkick dashboard provides an overview of infrastructure status; and graphs that help in visualizing bandwidth allowances and other metrics, as well as sends email alerts when things go wrong.

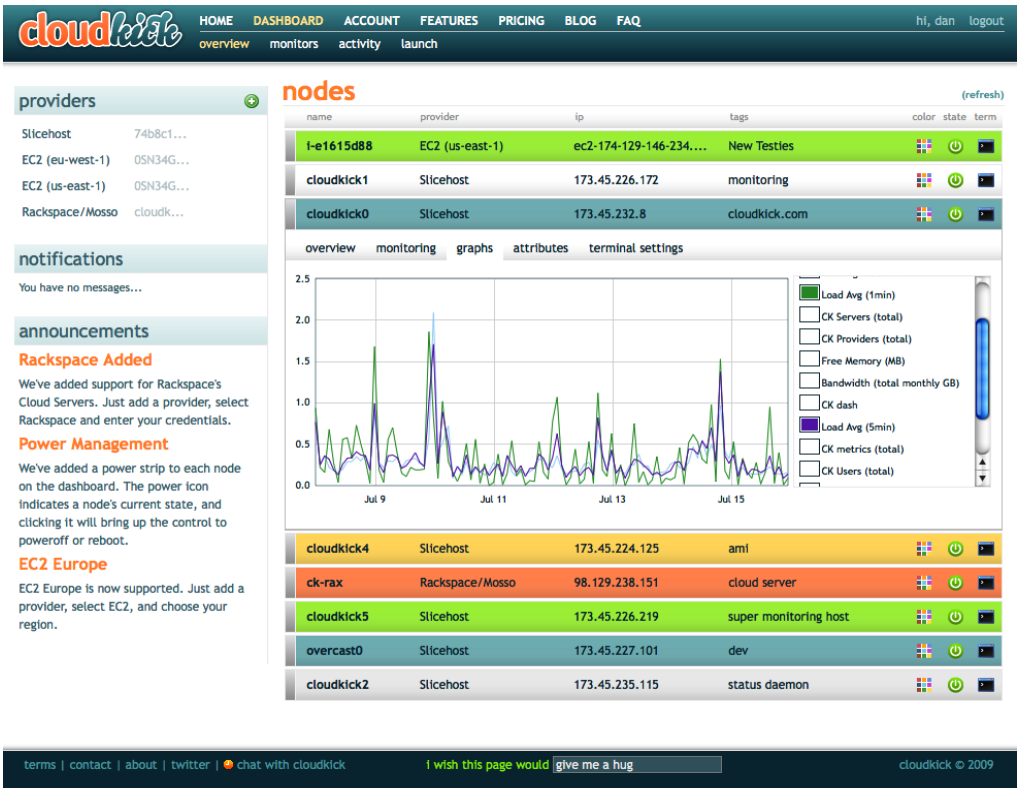

Fig 3:Snapshot of CloudKick Dashboard[14].

Thus tools which mainly focus on monitoring the user activities on cloud are required. Further, securing the logging information is very crucial from cloud forensics point of view [15-16],but providing security to the logging information i.e. evidence is very challenging in cloud environment, since clouds are not meant for security and forensics . Thus mechanism for storing the logs and making them available in a secured way are needed.

III. PROPOSED FRAMEWORK

1.3 Entities Used in the Architecture

1.3.1 User:

User access the cloud for storing his data and performing data computation, users further communicate with the trusted third party to get the required information. Users consist of both individual consumer and organizations.

1.3.2 Cloud Service Provider(CSP):

CSP has significant resources and expertise in building and managing distributed cloud storage servers, owns and operates live Cloud Computing systems

1.3.3 Trusted Third Party(TTP):

TTP is a trusted entity and has all the expertise and capabilities for maintaining users related information, and makes it available to user on behalf of CSP.

1.4 Architecture of Proposed Framework

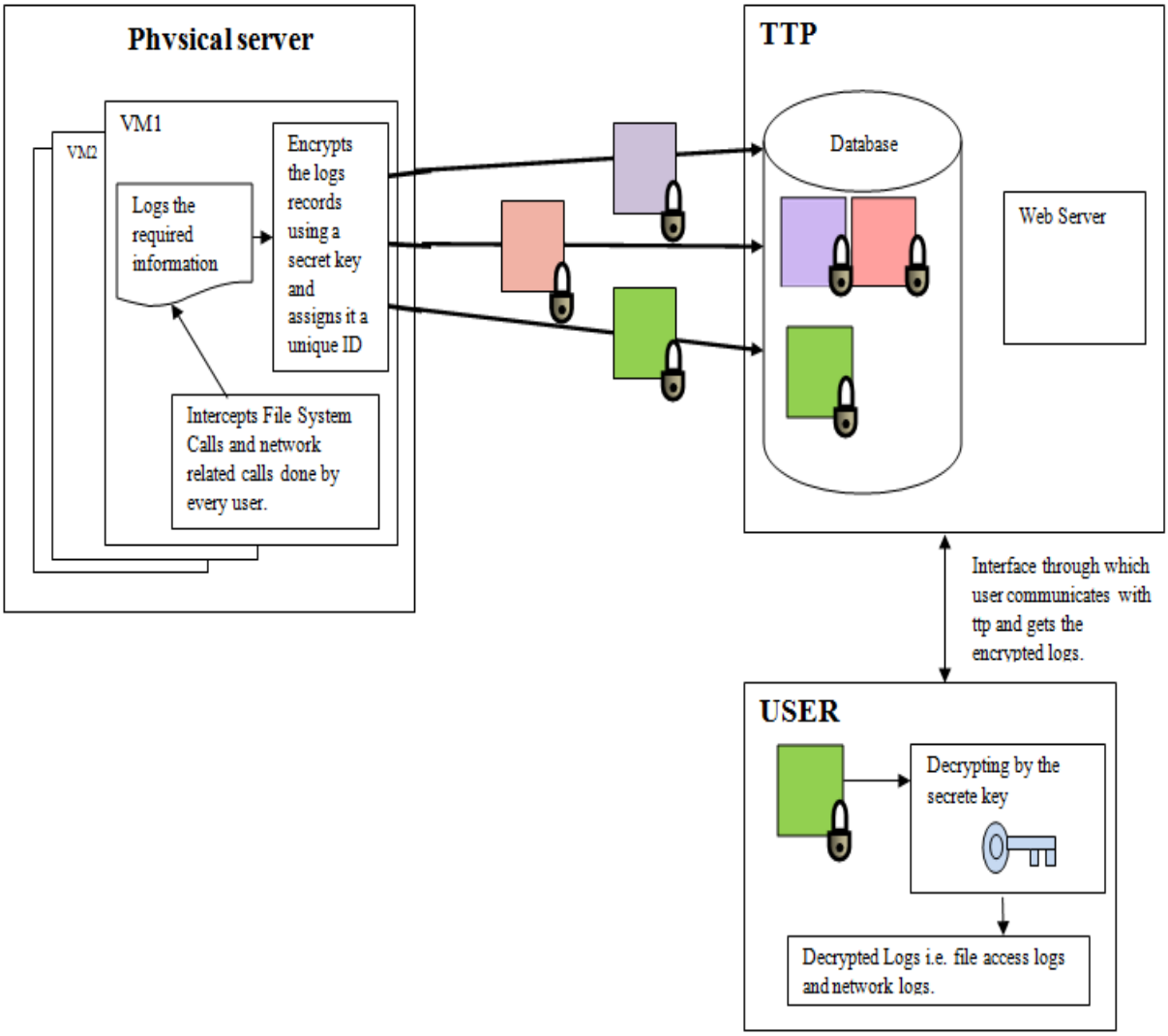

Fig 5:Proposed System

1.5 Logging Mechanism

For every user this mechanism records file-centric accesses, network access happening within the VM's, thus providing full transparency of entire user activities in the cloud. Basically two types of logs are maintained per user i.e. file access logs and network logs.

The following information is captured for every file access done on VM [8]:

- Process name who access the file.
- UID of process owner who accessed the file.
- GID of process owner who accessed the file.
- UID of file owner .
- GID of file owner .
- File owner name.
- File name and full path of file.
- VM IP address.
- VM MAC address.
- IP of underline physical machine.
- Time stamping information of file.
- Action done to accessed file e.g. create, read, write, delete, rename, socket(send message), socket(receive message).

Apart from the file access logs, network logs i.e. information about VM to VM communication and communication of VM with outside world is also captured. The network logs will stored the following information:

- UID of the user.
- GID of user.
- From IP.
- Remote IP.
- Remote port number.
- Timestamp information i.e. date and time.

The logs generated are further sent for the encryption purpose.

1.6 Kernel Level Encryption of Log Records

Logs generated are crucial to the entire cloud environment, hence they should be safeguarded. Since database in which the logs are stored comes under the CSPs architecture, there are chances that administrator or some malicious cloud employee can delete some log entries or can reorder the log entries or even add some fake entries to it. Thus it is suggest to involve a TTP who takes care of the log files. Controlling access to logs isn't really the most effective way to prevent loss or exposure of its contents. Thus a mechanism which protects the logs from the risks of losing or exposing is needed. Proposed framework supports encryption at kernel level. As soon as the logs records are generated, VM's encrypts it at the kernel level using the fastest and most advanced encryption algorithm. Further the kernel generates a unique system generated ID for every encrypted log record and transfers the log record to TTP for storage purpose. Kernel level encryption is more beneficial than user level encryption since the users, malicious insiders, hackers and even the CSP has no access to it.

1.7 Storing and Accessing Logs

It is not safe to store the logs in cloud environment since it can be accessed by CSP,cloud employee or other user.Thus,the proposed framework suggest the used of TTP i.e. trusted third party for storing and providing access to the logs.TTP stores logs in encrypted form for every user of CSP.Valid cloud user can get access to the logs on request by communicating with TTP. Log file provided to the user by TTP will be in encrypted form, user decrypts the file by using his private key(A pair of private and public key is given to each and every cloud user by TTP.Public key is made public whereas private key is kept secret by user).

1.8 Security Analysis

Logs are always generated by the CSP and maintained by TTP Thus, while transferring the logs to the TTP for storage, the CSP can tamper the logs .Such attempts for violating the integrity and confidentiality of logs can be easily detected by kernel level encryption .

Following presents the possible attacks on the logs and how the above discussed kernel level encryption defends these attacks.

1.8.1 Removal of crucial log information:

Since generation and encryption of logs happens at kernel level and as soon as the log record is encrypted it is moved out of cloud environment to TTP, making it almost impossible for anyone including CSP to access it.

1.8.2 Reordering of logs and inserting fake log information:

Since every encrypted log record is given a unique system generated ID, reordering attacks can be easily detected. The reorder log records ID's will be out of sequence. Further fake log records inserted can be detected since these fake log records won't have the unique system generated ID.

1.8.3 Privacy Preserving at TTP:

Since the log files stored at TTP are in encrypted form, TTP cannot infer any knowledge out of it.

IV. CONCLUSION

Current systems require that the user should completely trust the CSPs, which is not acceptable to many organizations. Thus, there is a need to develop mechanisms which will allow the organizations to monitor and assess the trustworthiness of CSP.In this paper we propose a framework which helps to increase trust in CSP. Users are made accountable for every activity done by them on cloud. Further the accountability information generated is vital for conducting auditing and cloud forensics. Thus a kernel level encryption mechanism is proposed by which, it is possible to encrypt the log. Further use of TTP is suggested for storing and providing access to logs. Accountability combined with secure logging will make clouds more reliable and trustworthy.

V. REFERENCES

[1] A. Haeverlen, and, "A Case for the Accountable Cloud",ACM SIGOPS Operating System Review,vol.44,pp.52-57,2010.

[2] C. Cachin, I. Keidar, A. Shaer, "Trusting the Cloud", ACM SIGACT News, vol.40, No.2, June 2009.

[3] K. L. Ryan Ko, P. Jagadpramana, M. Mowbray, S. perasons, M. Kirchberg, Q. Liang, B. S. Lee "TrustCloud-A freamework for accountability and trust in cloud computing",IEEE 2nd Cloud Forum for Practitioners,IEEE Computer Society, Washington DC, USA, 7-8 July 2011.

[4] Cloud Security Alliance," Top Threats to Cloud Computing(V1.0)",2010;https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

[5] J. K. Muppala,D. Shukla,S. K. Patil, "Establishing Trust in Public Clouds", J Inform Tech Softw Eng,2012.

[6] S. Zawoad, A. K. Dutta and R. Hasan, "SecLaas:Secure Logging-as-a-Service for Cloud Forensics", ACM Symposium on Information, Computer and Communications Security (ASIACCS) Feburary 25,2013.

[7] O. Q. Zhang, K. L. Ryan Ko, M. Kirchberg and B. S. Lee, "How to Track Your Data:The Case for Cloud Computing Provenance",January 21, 2012.

[8] K. L. Ryan Ko, P. Jagadpramana and B. S. Lee "Flogger:A File-centric Logger For Monitoring File Access and Transfer within Cloud Computing Environments",In Proc.IEEE 10th International Conference on Trust,Security and Privacy in Computing and Communication,pp.765-771 August 6,2011.

[9] S. Pearson and A. Charlesworth and, "Accountability as a Way Forward for Privacy Protection in the Cloud", Springer LNCS 5931, pp. 131–144, December 2009.

[10] S. Pearson, "Towards Accountability in the Cloud",IEEE Internet Computing, IEEE Computer Society, vol.15, no.4, pp. 64-69, July/August 2011.

[11] N. Michalakis,R. Soule and R. Grimm," Ensuring Content Integrity For Untrusted Peer to Peer Content Distribution Network",In Proc. NSDI,April 2009.

[12] A. Haeberlen, P. Kuznetsov, P. Druschel,"PeerReview:Practical Accountability for Distributed Systems",In Proc.SOSP,October 2007.

[13] HyTrust,"HyTrust Appliance",2010; http:/www.hytrust.com/product/overview/.

[14] CloudKick,"CloudKick-Cloud Monitoring and Management",2011; http:/www.cloudkick.com.

[15] D. Ma, G. Tsudik,"A New Approach to secure Logging",Trans.Storage,5(1):2:1,March 2009.

[16] R. Marty,"Cloud Application Logging For Forensics",In Proc. ACM Symposium on Applied Computing,pp 178-184,2011.

.

.