SECURING LOG AND DATA USING CLASS SCHEME IN CLOUD FORENSICS

Poornashree Nagesh[1], Dr. R Aparna[2]
[1]PG Student, Department of ISE, SIT, Tumkur, India.
[2]Professor, Department of ISE, SIT, Tumkur, India.

Abstract:

In cloud forensic investigations, activity logs are the valued source of information. So safeguarding the integrity and reliability of the logs is essential. The solutions of existing system for secure logging are planned in a way for conservative system rather than the complication of a cloud environment. In this paper, we used the CLASS scheme for the securing of logs and data in a cloud environment. The logs and data are encrypted in this process. To avoid the unauthorized modification of the log, we generated proof of past log for verification.

Keywords: Cloud computing, Data security, Cloud Forensics;

1. INTRODUCTION

Cloud computing is one of the emergent technology which uses the various services, such as software development platforms, storage, software, servers over the internet, often stated to as the cloud. It is a way of using a cluster of network through remote servers hosted on the internet as an alternative of local server or a personal computer to store, manage, and process data.

Cloud computing plays a vital role in enhancements of virtual platform and storage. Cloud is used by numerous customers. Cloud is divided into three categories as a Private Cloud, Public Cloud and Hybrid Cloud. Cloud computing services are divided into three categories as Infrastructure as a Service, Software as a Service and Platform as a Service. The cloud users will pay and use the cloud space for their workspaces and there many vendors who offers the services are Amazon Web Service, Microsoft Azure, SAP, Rackspace …etc.

The Cloud Security is also well-known as a Cloud Computing Security is one of the rapidly increasing service that affords many functionalities. This protects the confidential information from data theft, data leakage, attacks and deletion. It also offers the protection of data, applications, and infrastructures involved cloud computing. In computing environment, cloud security includes maintaining satisfactory preventative protections.

Digital Forensics is one of the division of forensic science and procedure is to discovery and interpreting the electronic data because to preserve the evidence and performs a collecting, identifying and validating the information or data found on computers or storage devices. The Investigator has to be answer some of the queries when the crime or an incident is occurred like 'why, how, who, what, where and when'.

The Cloud technologies are updating frequently their features, sequentially we have to update our digital forensics tools for the effectiveness and pertinence in cloud computing environment.

In a collected environment the virtual machines are distributed in many physical devices or in group of virtual machines on same devices they can be exist. So this type of devices for investigations is not possible in forensic examination. The data in a virtual machines are unstable, the data will loss once the power is off or if the device is terminates. The vital role in group of data is plays by the cloud service provider because the cloud service provider captures the activity logs of each user and this prevents the alteration of the logs and have to assure the privacy of the data because it plays a key role. The activity logs stored in the computer is belongs to a specific user and this conserves the confidentiality and also helps in the investigation events.

The S. Zawoad, A. K. Dutta, and R. Hasan [7], proposed SecLaaS is a secure logging as a service is planned in such a way that to collects data from one or more log sources, audit the data and stores the data in a dedicated storage to avoid the risk. While storing the data, the logs are encrypted and also produces the log chain to obtain the confidentiality and integrity. In Secure Logging as a Service the logs are encrypted using the investigator public key and the encrypted logs are stores in a cloud server. To achieve integrity, the proof of past log (PPL) is generated with a log chain in Secure Logging as a Service and publish it publically at definite period. This PPL also supports to minimize risks in cloud by reducing the dishonest user altering the log and also helps for the investigation. But in SecLaaS have certain limitations in accountability and transparency. Extending SecLaaS, the Cloud Log Assuring Soundness and Secrecy (CLASS) scheme is designed in such a way that to ensure the cloud service provider accountability

and the user privacy preservation and also user can validate their accuracy of the log. The PPL is generated using Rabin's fingerprint and bloom filter.

2. RELATED WORK

In forensic investigations the cloud logs plays a very important role to preserve the confidentiality, integrity and forward secrecy, validating the verification and availability by authorized party are it should be taken care by the investigator. Anwar et al [8] addressed the syslog or snort log which identifies the cloud attacks. The authors of this paper conducted the analysis of the investigation by generating logs using a Eucalyptus it is an open source software. The authors generated their own dataset via doing DDos on software and they also identified the attacked IP address of the machine.
The log management scheme is proposed by the Schneier and Kelsey [4] based on forward integrity. This authors ensured that using of secret key for MAC and one-way hash chain rather than pseudo random function. This type of scheme requires for online trusted user to maintain and verifies the secret key and integrity. Holt [2] proposed the remove of essential of online trusted server using a public key cryptography. Zawoad et al [7] proposed the Secure logging as a Service this has collected the flaws in CSP's like a volatility, multiple users cloud data and also malicious loggers. The authors provided the solution of secure logging for all the cloud actions in virtual machines.

3. THREAT MODEL

The Proposing scheme is designed like a 'trust no one'. The cloud service provider, user and investigator will able to protect their own security and privacy against between a parties. For example modification of log, the dishonest cloud service provider will issues the logs before publishing the logs and it can be modified by CSP or by an fraudulent investigator can be modify the logs before submitting in front of court. The privacy violation is an example, the privacy information can be leakages by sharing the log file it can expose the information of the users.

4. SECLASS

In Secure Logging as a Service the scheme which proposes a robust and effective technique for cloud log management, by gathering the logs and prepare the proof by using collected logs and that proof will be publicly accessible and also it protects their privacy, integrity and forward secrecy. This scheme reserves the encrypted logs in storage and later it produces the proof and publish its proof that not be alter by any party.
SecLaaS has some boundaries that are Privacy violation and Adulterating log before publishing. The privacy violation of user will happens by collusion between the cloud and investigator. In this scheme the logs are stored in the database by encrypting it with law enforcement public key so that no one apart from authority can decrypt it. However the person who knows the key of the investigator agency may join with the malicious cloud provider and they can disclose the data some portion or the entire data in database then privacy of the user is compromised. Next one is a altering the log before publish of the proof of past log. In the existing scheme it only supports for the altering or modification of the logs after publishing the PPL.

5. PROPOSED SCHEME

This scheme is designed like a 'trust no one' in the cloud infrastructure i.e., an attack may be come from user, cloud service provider or an investigator. A mischievous user can attack the system in cloud from outside the cloud it may cause like the applications deployed in the cloud may be attacked or they may attack a node controller
which supports for all the activities in the cloud. For example in this CLASS scheme collects the log from the node controller in virtual machine and encrypts its content, stores it in the database and publishes the proof of past log which may useful for the investigations if anything happens in the cloud. The Scheme publishes the proof so the integrity of the data is protected.

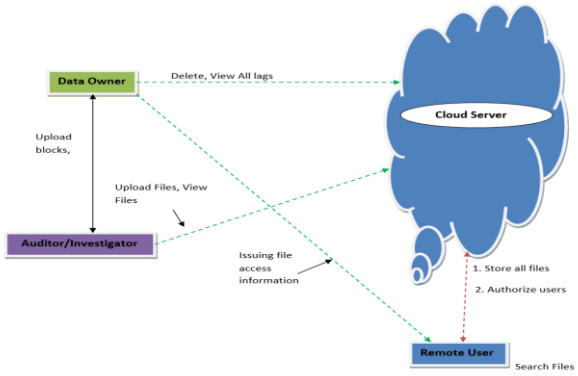

Fig 1: Architecture

In this paper, the CLASS scheme deals with the security of the data which is shared by owners within the cloud. In this methodology we are working on four models that are user, CSP, data owner and the Investigator. The data owner and the users first they have to register with the cloud for uploading the data to the cloud and for users to download the file they have to register first. The registration form is built in the form there people have to enter their personal information and register to use the cloud. After the registration the data owner and user details sent to the cloud service provider. The CSP should authorize or grant the access for the data owner and user. The CSP have to grant an access by knowing the data owner and user is a correct person and details entered by the data owner and the user while registration is correct. When the data owner wants to upload a file to the cloud, they just attach a file which is to be upload and the encryption takes place in this scheme I am using the symmetric algorithm for the encryption and the decryption. Using the same key the data is encrypted and for decryption the same key is used in the other side. For user whenever they wants to download a file, first they have to register after they have to request the access for the search a file by using their credentials, this access should be gives by the cloud service provider. When the CSP provides the access for search then user can move to search a file which they want to download. Later when users wants to download the file they have to click on the download icon and next they have to request for the key to cloud service provider to download a file. The cloud service provider will provide the secret key if the user is authorized otherwise cloud service provider will not provide the key details. By entering the correct key details users can download a file. For security perspective the data in the cloud and the timestamps captured when uploading and downloading the file information is encrypted, the CSP can't know anything in the cloud. The proof of past log is generated and it will publish to the internet, where investigator can login and verifies the log and data information if anything wrong happens in the cloud or if data owner thinks that the data theft, modification of data happens or any attacks to cloud. The investigator is belongs to a government agency or a private organization. They verify the logs comparing with a proof of past log.

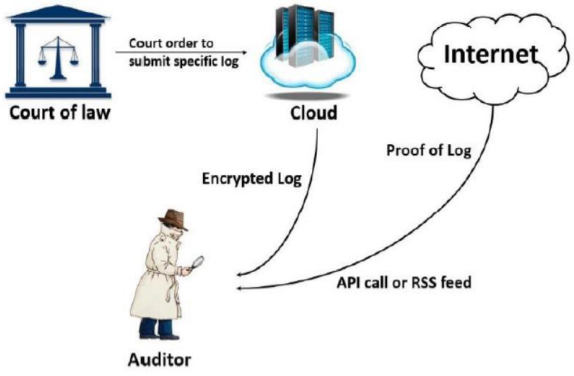

Fig 2: Overview of verification process

The above figure 2 shows the verification process, this process only establish the authenticity and also determine if any contamination in log. There are two types of process to verification in this project. First is where we have to checks that CSP is writing correct log entries or not. In second verification is by investigator or law enforcement authority or a court of law to verify the proof of past log to check is there any changes or modification in logs.

The figure 3 shows the sequence diagram of process. In our model we have data owner, remote user, cloud service provider and investigator. The data owner will upload a files by encrypting and the logs will publishing

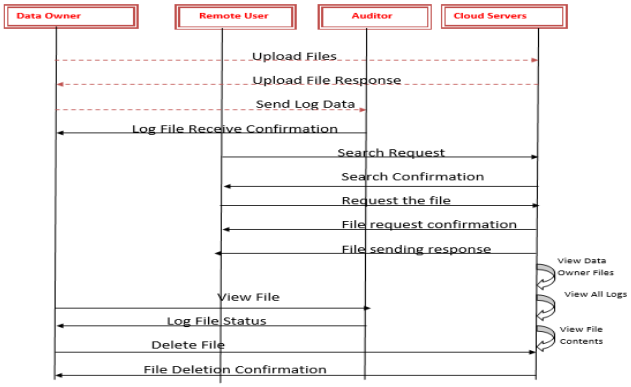

Fig 3: Sequence diagram

6. RESULTS

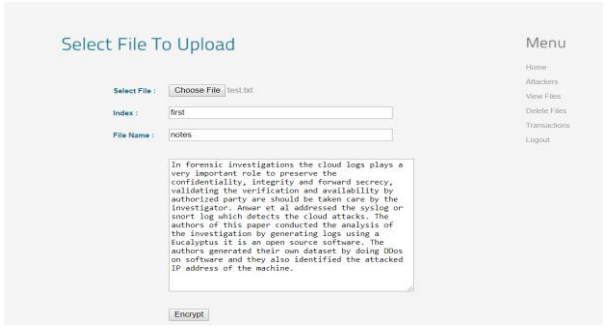

Fig 4: Data owner uploading a file

In figure 4 data owner wants to upload file, they have to select file by clicking choose file option, then data owner have to enter an index and file name later they have to click on a encrypt option.

Fig 5: Encryption of uploading file

The selected file from the data owner is encrypted and it will upload by clicking on the upload option. If the data is uploaded then it comes data successfully uploaded.

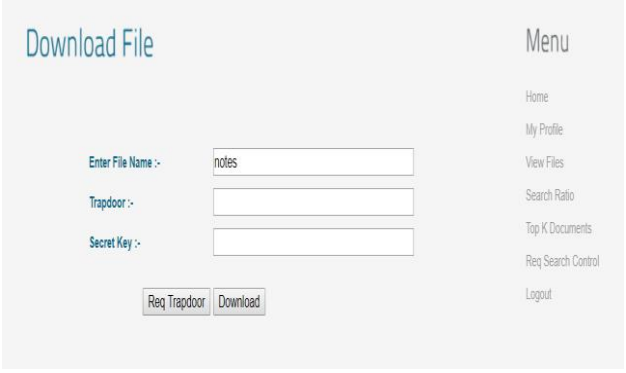

Fig 6: User request for trapdoor

The user will have to request a trapdoor to download a file by clicking the Req Trapdoor

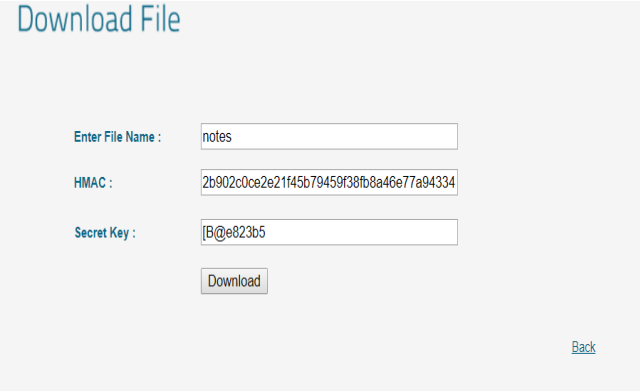

Fig 7: The secret key is generated

If the secret key and HMAC matches then only user can able to download a file by clicking on download icon. Otherwise the secret key mismatch will come and user will unable to download a file, this just like an OTP.

Fig 8: List of attackers

The data owner can see that the unauthorized person who tried to download a file with a timestamp and the mismatch key using whose username.

7. CONCLUSION

In this paper, we proposed a secure logging scheme for cloud computing with features that simplify the preservation of user privacy and also it that alleviate the effects of collusion between the other parties. The CLASS scheme conserves the privacy of cloud users by encrypting cloud logs and information/file of the corresponding user while also simplify the log retrieval in the event of an investigation. Additionally, it certifies accountability of the cloud server by permitting the user to identify any log modification. This has the additional outcome of preventing a user from repudiating entries and it is difficult to modify the log once the PPL is established. The experimental results show an enhancement in effectiveness thanks to the features of the CLASS scheme, particularly in verification phase.

REFERENCES:

[1] M A Manazir Ahsan, Ainuddin Wahid Bin Abdul Wahab, Mohd Yamani Idna Bin Idris,"CLASS: Cloud Log Assuring Soundness and Secrecy Scheme for Cloud Forensics" IEEE Transactions on Sustainable Computing
[2] J. E. Holt, "Logcrypt: forward security and public verification for secure audit logs," in Proceedings of the 2006 Australasian workshops on Grid computing and e-research-Volume 54, 2006, pp. 203-211.
[3] Q. Alam, S. U. Malik, A. Akhunzada, K.-K. R. Choo, S. Tabbasum, and M. Alam, "A Cross Tenant Access Control (CTAC) Model for Cloud Computing: Formal Specification and Verification," IEEE Transactions on Information Forensics and Security, vol. 12, pp. 1259-1268, 2017.

[4] B. Schneier and J. Kelsey, "Secure audit logs to support computer forensics," ACM Transactions on Information and System Security (TISSEC), vol. 2, pp. 159-176, 1999.
[5] C. Hooper, B. Martini, and K.-K. R. Choo, "Cloud computing and its implications for cybercrime investigations in Australia," Computer Law & Security Review, vol. 29, pp. 152-163, 2013.
[6] S. Khan, A. Gani, A. W. A. Wahab, M. A. Bagiwa, M. Shiraz, S. U. Khan, et al., "Cloud log forensics: foundations, state of the art, and future directions," ACM Computing Surveys (CSUR), vol. 49, p. 7, 2016.
[7] S. Zawoad, A. K. Dutta, and R. Hasan, "Towards building forensics enabled cloud through secure logging-as-a-service," IEEE Transactions on Dependable and Secure Computing, vol. 13, pp. 148-162, 2016.
[8]F. Anwar and Z. Anwar, "Digital forensics for eucalyptus," in Frontiers of Information Technology (FIT), 2011, 2011, pp. 110-116.
[9] X. Liu, R. H. Deng, K.-K. R. Choo, and J. Weng, "An efficient privacy-preserving outsourced calculation toolkit with multiple keys," IEEE Transactions on Information Forensics and Security, vol. 11, pp. 2401-2414, 2016.