International Journal of Research in Engineering, Science and Management
Volume-2, Issue-11, November-2019
www.ijresm.com | ISSN (Online): 2581-5792

Cloud Computing Assuring Secured Log System for Cloud Forensics

D. Ramanathan[1], G. Elizabeth Rani[2]

[1]UG Student, Department of Computer Science and Engineering, Kalasalingam Academy of Research and Education, Virudunagar, India

[2]Assistant Professor, Department of Computer Science and Engineering, Kalasalingam Academy of Research and Education, Virudunagar, India

***Abstract*: User activity logs can be a valuable source of information in cloud forensic investigations; hence, ensuring the reliability and integrity of such logs is crucial. Most existing solutions for secure logging are designed for conventional systems rather than the complexity of a cloud environment. In this project, we propose the Cloud Computing Assuring Log System for Cloud Forensics process as an alternative scheme for the securing of logs in a cloud environment. In Cloud, logs are encrypted using the individual user's public key so that only the user is able to decrypt the content. In order to prevent unauthorized modification of the log, we generate proof of past log (PPL) using user fingerprint and Attribute Based algorithm. Such an approach reduces verification time significantly.**

***Keywords*: Cloud forensics, Encrypted, Decrypted, Fingerprint, Attribute Based.**

1. Introduction

Cloud storage, security and privacy are fairly established research areas, which is not surprising considering the widespread adoption of cloud services and the potential for criminal exploitation (e.g. compromising cloud accounts and servers for the stealing of sensitive data). Interestingly though, cloud forensics is a relatively less understood topic.[1] In the event that a cloud service, cloud server, or client device has been compromised or involved in malicious cyber activity (e.g. used to host illegal contents such as radicalization materials, or conduct distributed denial of service (DDoS) attacks) , investigators need to be able to conduct forensic analysis in order to “answer the six key questions of an incident – what, why, how, who, when, and where”.[2] Due to the inherent nature of cloud technologies, conventional digital forensic procedures and tools need to be updated to retain the same usefulness and applicability in a cloud environment The basis of both schemes relies on the fact that, keeping a small and secret piece of information with each log entry which cannot be generated without a secret key, and this secret key changes with each new log. With this secret information, a log entry can be verified later on for its integrity. [3] However, such schemes require the presence of an online trusted server to maintain the secret key and to verify its integrity.

2. Literature review

Dweepayan Mishra et. al. proposed in his paper that few works are being carried out for automated irrigation system. Some research works mentioning that various algorithms and different microprocessor used for their results. Several scientists have worked with water system framework or programmed water sprinkling. They selected individual measurements for determining the amount of water and soil condition. Various wellsprings of energy for the sensors they are examined. Plus, the novelty for making system among the sensors and outline of control framework was moreover deeply analyzed by researchers. [4]

The aim of this system is to modernize farming innovation by using programming segments and construct the necessary parts for the framework. The framework is ceaseless based and focuses the right condition of paddy field. There is one central center used which to control another center. The key limit of RF module is to pass the message to the center point and work the system.

3. Existing system

- The existing system provides a on demand network access for the users to configure over a shared pool of resources which means is an open log access with an easy accessibility of data criterian.
- A malicious investigator may alter the log before presenting to court to save a dishonest user or to frame a honest user [5].
- Though the data have quite common interface environment it was sentenced for maximal data leakage with the user’s service provision.
- The cloud logs system rapidly released with minimum percentage of management effort of provider service.

4. Issues in existing system

The data is stored away from the owner which increases the vulnerability of the information. The existing systems does not have the regular audits that can cause leakage of data or lacking in information theft. Since it has varied dimensions of computer resource such as cross borders and etc. requires extra secured system for analyzing and managing the information at regular intervals.

Service providers face a situation to set up or enable data centers for large number of users to store their data efficiently. [5] Every service has their own implementation of all the technical layers which differentiates their standard with another. [6]

5. Proposed system

The proposed framework consists of logging scheme, provides a protected log file handling, to design to ensure accountability and preserve the user's privacy. Specifically, it includes the capability for the user to verify the accuracy of their log.

To do this, the log will be encrypted using the user's public key (other than the agency's public key). provides extra secured system for analyzing and managing the information at regular intervals. The proposed system prevents data leakage in high percentage. [7]

6. Methodology

- To have a safe logs in cloud registrations, the logs are encrypted using the individual user's public key so that only the user is able to decrypt the content.
- Also to generate proof of past log content using Fingerprint and Attribute Based algorithm.
- Cloud server is connected to where the information is sent and received according to the proposed user request.
- The retrieved has the parts originating from different servers to protect the data securely and for the purpose of preserving the data efficiently. [8]

7. Modules description

- *Investigator:* In this module, investigator will register it and then they will get password. According to the password they will navigate to the next page. Investigator will give the request to the cloud service provider. Currently investigator will monitor their request status. If the investigator want to view the log file details that also possible. Finally, investigator find the file details.
- *CSP:* In this module, cloud service provider may want to view user request that will happened from the cloud. Continuously, cloud service provider view user details and investigator request. If some user need to change their file. cloud service provider will give the permission to that user. Finally, cloud service provider views the chart. In that chart will display how many users will download the file.
- *Cloud:* In this module, cloud can hold the uploaded file which are uploaded by admin and cloud can handle shared file and deleted file status. At the end, cloud admin will view all file details which are available in cloud.
- *User:* In this module, user first register it. According to the registration they will get password. Through that password they will view cloud server plan details and request plan details. Finally, user may want to download the file that also possible.

8. System design

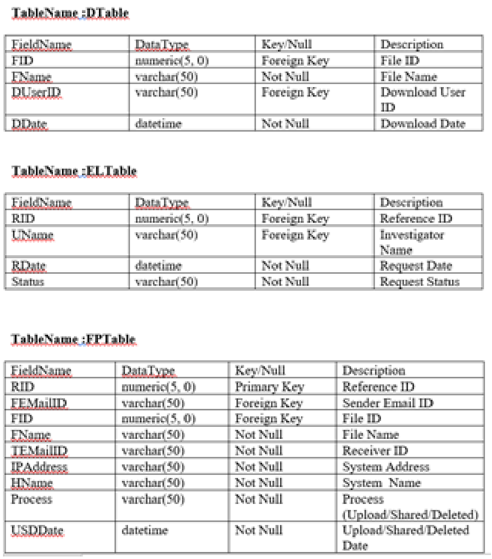
A. Input Design

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. [9]

B. Output Design

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making. [10]

- Trigger an action.
- Confirm an action.
- Database Design



TableName :DTable

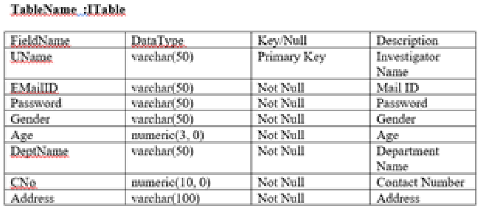
FieldName	DataType	Key/Null	Description
FID	numeric(5, 0)	Foreign Key	File ID
FName	varchar(50)	Not Null	File Name
DUserID	varchar(50)	Foreign Key	Download User ID
DDate	datetime	Not Null	Download Date

TableName :ELTable

FieldName	DataType	Key/Null	Description
RID	numeric(5, 0)	Foreign Key	Reference ID
UName	varchar(50)	Foreign Key	Investigator Name
RDate	datetime	Not Null	Request Date
Status	varchar(50)	Not Null	Request Status

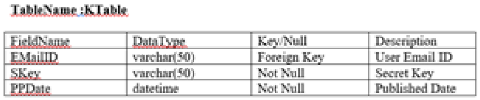
TableName :FPTable

FieldName	DataType	Key/Null	Description
RID	numeric(5, 0)	Primary Key	Reference ID
FEMailID	varchar(50)	Foreign Key	Sender Email ID
FID	numeric(5, 0)	Foreign Key	File ID
FName	varchar(50)	Not Null	File Name
TEMailID	varchar(50)	Not Null	Receiver ID
IPAddress	varchar(50)	Not Null	System Address
HName	varchar(50)	Not Null	System Name
Process	varchar(50)	Not Null	Process (Upload/Shared/Deleted)
USDDate	datetime	Not Null	Upload/Shared/Deleted Date



TableName :ITable

FieldName	DataType	Key/Null	Description
UName	varchar(50)	Primary Key	Investigator Name
EMailID	varchar(50)	Not Null	Mail ID
Password	varchar(50)	Not Null	Password
Gender	varchar(50)	Not Null	Gender
Age	numeric(3, 0)	Not Null	Age
DeptName	varchar(50)	Not Null	Department Name
CNo	numeric(10, 0)	Not Null	Contact Number
Address	varchar(100)	Not Null	Address

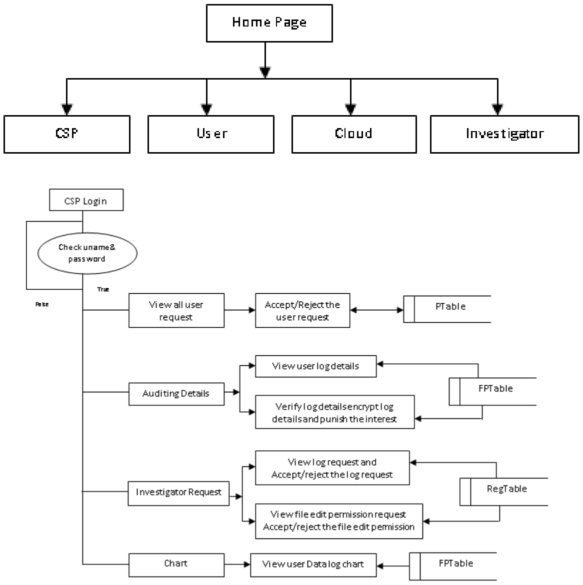


TableName :KTable

FieldName	DataType	Key/Null	Description
EMailID	varchar(50)	Foreign Key	User Email ID
SKey	varchar(50)	Not Null	Secret Key
PPDate	datetime	Not Null	Published Date

9. Work flow – chart

.NET based Cloud Log system includes a blocks of login servers, in order to process and authenticate the user for safe login with its details.



Home Page
CSP
User
Cloud
Investigator
CSP Login
Check uname& password
True
False
View all user request
Accept/Reject the user request
PTable
View user log details
Auditing Details
FPTable
Verify log details encrypt log details and punish the interest
View log request and Accept/reject the log request
Investigator Request
RegTable
View file edit permission request Accept/reject the file edit permission
Chart
View user Data log chart
FPTable

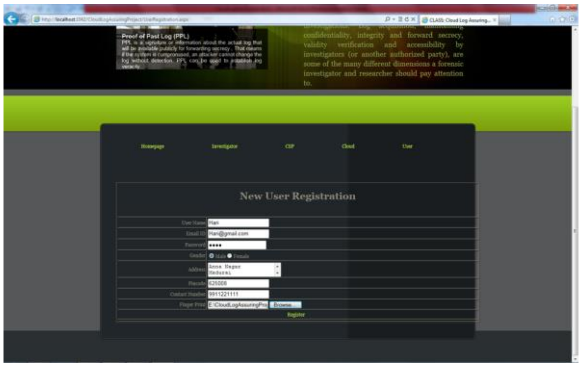
Fig. 1. Flowchart of process used

10. System implementation

Implementation is the stage in the project where the theoretical design is turned into a working system. The most critical stage is achieving a successful system and in giving confidence on the new system for the users, what it will work efficient and effectively. It involves careful planning, investing of the current system, and its constraints on implementation, design of methods to achieve the changeover methods. [11] The implementation process begins with preparing a plan for the implementation of the system. According to this plan, the activities are to be carried out in these plans; discussion has been made regarding the equipment, resources and how to test activities.

The coding step translates a detail design representation into a programming language realization. Programming languages are vehicles for communication between human and computers programming language characteristics and coding style can profoundly affect software quality and maintainability. [12]

11. Result



http://localhost:1942/CloudLogAssuringProject/UserRegistration.aspx
CLASS: Cloud Log Assuring...
Homepage
Investigator
CSP
Cloud
User

Proof of Past Log (PPL)

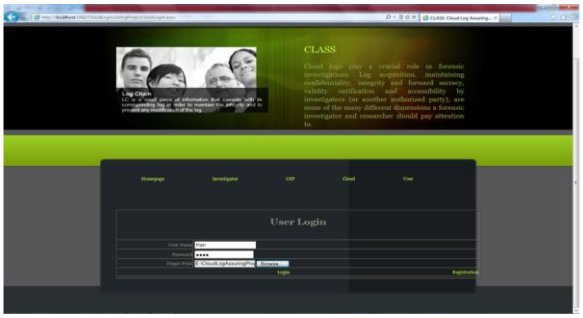
PPL is a signature or information about the actual log that will be available publicly for forwarding secrecy. That means if the system is compromised, an attacker cannot change the log without detection. PPL can be used to establish log veracity.

confidentiality, integrity and forward secrecy, validity verification and accessibility by investigators (or another authorized party), are some of the many different dimensions a forensic investigator and researcher should pay attention to.

New User Registration

User Name: Hari
Email ID: Hari@gmail.com
Password: ****
Gender: ○ Male ● Female
Address: Anna Nagar Madurai
Pincode: 625008
Contact Number: 9911221111
Finger Print: E:\CloudLogAssuringPro Browse...
Register

Fig. 2. New user registration



http://localhost:1942/CloudLogAssuringProject/UserLogin.aspx
CLASS: Cloud Log Assuring...
Homepage
Investigator
CSP
Cloud
User

CLASS

Cloud logs play a crucial role in forensic investigations. Log acquisition, maintaining confidentiality, integrity and forward secrecy, validity verification and accessibility by investigators (or another authorized party), are some of the many different dimensions a forensic investigator and researcher should pay attention to.

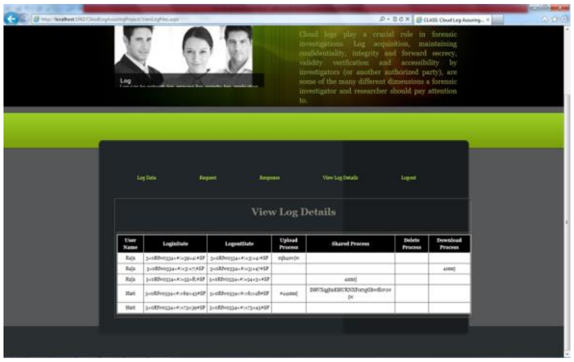
Log Chain

LC is a small piece of information that consists with its corresponding log in order to maintain the integrity and to prevent any modification of the log.

User Login

User Name: Hari
Password: ****
Finger Print: E:\CloudLogAssuringPro Browse...
Login
Registration

Fig. 3. User login



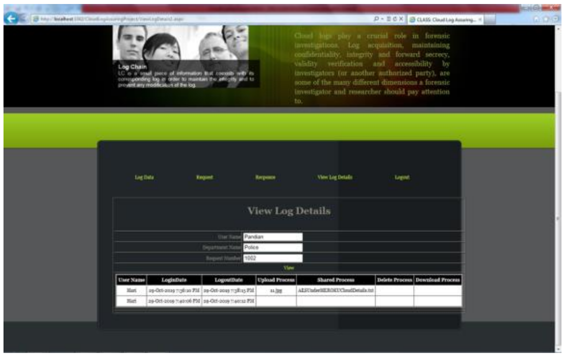
http://localhost:1942/CloudLogAssuringProject/ViewLogFiles.aspx
CLASS: Cloud Log Assuring...
Log Data
Request
Response
View Log Details
Logout

Cloud logs play a crucial role in forensic investigations. Log acquisition, maintaining confidentiality, integrity and forward secrecy, validity verification and accessibility by investigators (or another authorized party), are some of the many different dimensions a forensic investigator and researcher should pay attention to.

View Log Details

User Name	LoginDate	LogoutDate	Upload Process	Shared Process	Delete Process	Download Process
Raja	[illegible]	[illegible]	[illegible]			
Raja	[illegible]	[illegible]				[illegible]
Raja	[illegible]	[illegible]		[illegible]		
Hari	[illegible]	[illegible]	[illegible]	[illegible]		
Hari	[illegible]	[illegible]				

Fig. 4. Encrypted format of Log details



http://localhost:1942/CloudLogAssuringProject/ViewLogDetails.aspx
CLASS: Cloud Log Assuring...
Log Data
Request
Response
View Log Details
Logout

Cloud logs play a crucial role in forensic investigations. Log acquisition, maintaining confidentiality, integrity and forward secrecy, validity verification and accessibility by investigators (or another authorized party), are some of the many different dimensions a forensic investigator and researcher should pay attention to.

View Log Details

User Name: Pandian
Department Name: Police
Request Number: 1002
View

User Name	LoginDate	LogoutDate	Upload Process	Shared Process	Delete Process	Download Process
Hari	29-Oct-2019 7:36:10 PM	29-Oct-2019 7:38:15 PM	11.jpg	AESUnderHEROKUCloudDetails.txt		
Hari	29-Oct-2019 7:40:06 PM	29-Oct-2019 7:40:12 PM				

Fig. 5. Investigator view in decryption format

12. Conclusion

We proposed a secure logging scheme for cloud computing with features that facilitate the preservation of user privacy and that mitigate the damaging effects of collusion among other parties. Cloud preserves the privacy of cloud users by encrypting cloud logs with a public key of the respective user while also facilitating log retrieval in the event of an investigation. Moreover, it ensures accountability of the cloud server by allowing the user to identify any log modification. This has the additional effect of preventing a user from repudiating entries in his own log once the log has had its Past log details established. Our implementation on Open Stack demonstrates the feasibility and practicality of the proposed scheme.

13. Future enhancement

Thus, designing secure and efficient searchable encryption would extend this work. There is also the need for an online credibility system designed to develop trust and credibility of a cloud user so that the CSP can enable stricter auditing policies for low-trust users in comparison to high-trust users. Designing and implementing a prototype of the proposed scheme in collaboration with a real world CSP, with the aim of evaluating its utility (e.g. performance and scalability) in a real-world environment. proposed scheme in collaboration with a real world CSP, with the aim of evaluating its utility (e.g. performance and scalability) in a real-world environment.

References

[1] J. Zeng, T. Wang, Y. Lai, J. Liang, and H. Chen, "Data delivery from WSNs to cloud based on a fog structure," in Proc. Int. Conf. Adv. Cloud Big Data, 2016, pp. 104 –109.

[2] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement," IEEE Trans. Parallel Distribution. Syst., vol. 27, no. 9, pp. 2546–2559, Sep. 2016.

[3] Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, "An efficient public auditing protocol with novel dynamic structure for cloud data," IEEE Trans. Inf. Forensics Security, vol. 12, no. 10, pp. 2402–2415, Oct. 2017.

[4] M. Z. A. Bhuiyan, T. Wang, T. Hayajneh, and G. M. Weiss, "Maintaining the balance between privacy and data integrity in internet of things," in Proc. Int. Conf. Manage. Eng., Softw. Eng. Serv. Sci., 2017, pp. 177–182.

[5] R. Steinberg, "A geometric approach to the representations of the full linear group over a galois field," Trans. Amer. Math. Soc., vol. 71, no. 2, pp. 274–282, 1951.