International Journal of Research
ISSN: 2348-6848 Vol-3, Special Issue-6
National Conference on Recent Engineering Trends
NCRET- 2016
Held on 16th March 2016 organized by Institute of Knowledge College of Engineering, Pune, India.

A Log-based Approach Access Secure File to Make Digital Forensics Easier on Cloud Computing

Gundecha Nilesh
nil.gundecha@gmail.com

Supekar Namdev
namdevsupekar@gmail.com
Ransing Kailas
Kailasransing92@gmail.com
Bhambure Ratnadip
Ratnadip143@gmail.com
Prof.Ritesh Thakur
hod_comp_iok@yahoo.com

SP'sInstitute of Knowledge College Of Engineering, Department of computer engineering,

Savitribai Phule Pune University

Year 2016-17

International Journal of Research
ISSN: 2348-6848 Vol-3, Special Issue-6
National Conference on Recent Engineering Trends
NCRET- 2016
Held on 16th March 2016 organized by Institute of Knowledge College of Engineering, Pune, India.

Abstract:-

Cloud computing is law means Cloud computing raises some unique law enforcement concern regarding the location of prospective digital evidence, its protection and its subsequent forensic investigation. For instance if a customer or business becomes the target of a criminal investigation. They could move from one country to another country, their working environment to a cloud environment. This would offer a means for the business to continue its routine operations while the migrated environment is forensically examined. However, this is not without threat. data can be stored somewhere in the world. Its sharing could be to several location or country. Where privacy laws are different in each country. Establishing a chain of detention for the data would become difficult or impossible if its veracity and authenticity cannot be fully determined there are also potential forensic issues when the customer or user exits a cloud application. In the proposed system, approach which using logs model to building a forensic-friendly system. Using this model we can quickly collect information from cloud for some kinds of forensic purpose and this will decrease the complexity of those kinds of forensics

Keywords: Cloud computing; Forensics; log

I Introduction:

In Cloud Computing During a digital investigation, forensic analysts are used to performing queries, indexing data, calculating hashes, extracting features and correlating partial data to narrow the search and solve the case. As long as investigation complexity, on the one hand, and amount of data to analyze, on the other, allowed it, forensic data processing occurred in sequence on stand- alone forensic workstations. Unfortunately, Internets pervasiveness and market availability for cheap and sophisticated mobile devices with large storage capacity, have changed the landscape, resulting in an increase of digital investigation complexity and contributing to the global diffusion of cybercrimes as well. Such crimes, on the one hand, are evolving at an amazing pace, following the same dynamic as the inevitable penetration of computer technology and communication into everyday life. At the same time as society is inventing and developing, at the same time, criminals are deploying a remarkable adaptability in order to derive the greatest benefit from it. Digital forensics, as an effect, seems to be facing new challenges which, if not taken seriously, may rapidly render the actual forensics techniques obsolete and even not practicable. Cloud computing accesses secure file is important to use in crime investigation

II. TECHNOLOGY

BACKGROUND

1 Cloud Computing

Cloud computing which is also known as Internet computing generally is seen as collection of clouds on the web. International It provides technology enabled services to the people and organizations by utilize the internet. People can just access to the web anywhere and at any time without to think about the corporal management as well as the maintenance issues. Most of the cloud computing resources are very dynamic and scalable because they are independent computing which is free from maintenance cost. The most widely used definition of cloud computing is made by NIST where they define Cloud Computing as a pool of computing resources such as servers, networks, services and applications that provide expediency, flexibility and more performance on order network access which is consisting of five essential characteristics, three service models and four deployment models.

Digital Forensics

Digital forensics is also known as computer forensics or computer forensics is the process of

preparing, purchase, preserving, examining and analyzing and also reporting of digital data. The purpose of this digital forensics is to improve and to obtain legal evidence found in digital media. According to the NIST, the current definition of digital forensics is the scientific procedures used to identify and classify, collect, evaluate, and analyze the data while maintaining the level of integrity of the information throughout the forensics process[3].

The purposes of digital forensics are including forensic computing, forensic calculations and computer forensics. Being called into official proceedings is one of the digital forensics risks. Thus it must have a correct procedure in conducting the forensic investigation and doing the check setup where this procedure or tactic must basically base on the scientific principles. Although several studies had been done and the objectives more focused on the technical issues, challenges and the opportunities, but there is still a needed to do further research and find the most effective methods to evaluate particularly the uncertainty of the evidence or any forensic findings in the cloud forensics processes. Forensic investigators need to fulfill themselves with a multiple disciplines of knowledge in order to investigate the digital evidence in a cloud environment. They need to master specific areas such as mobile, hard disk, registry and others that can be presented in court as legal evidence since all these evidences are in a virtual manner, not as others physical evidences. In order to ease the tasks of identifying before the extract to analyze the evidences, a reliable and specialize frameworks, tools, applications and other forensic requirements are needed. This paper will focus on the cloud forensics environments including the basic framework and design, the challenges and opportunities and also the security issues. It will further discuss the forensic investigations when it include into the cloud computing environment that covers from the digital evidence, the framework, the implication of digital investigations to the cloud computing environment and others.

III. CHALLENGES FOR CLOUD FORENSICS

Digital investigations are about control of forensic evidence data. From the technical position, this data can be available in three different states: at rest, in motion or in execution. Data at rest is represented by allocated disk space. Whether the data is stored in a database or in a specific file format, it allocate disk space. also, if a file is deleted, the disk space is de-allocated for the operating system but the data is still available since the disk space has not been re-allocated and overwritten. This fact is often oppressed by investigators which explore these de-allocated disk space on hard disk. In case the data is in motion, data is transfer from one entity to another e.g. a typical file transfer over a network can be seen as a data in motion condition. Several encapsulated protocols contain the data each leaving specific traces on systems and network devices which can in return be used by investigators[1].

Data can be loaded into memory and executed as a process. In this case, the data is neither at rest nor in motion but in execution. On the executing system, process information, machine instruction and allocated/deallocated data can be analyzed by creating a snap of the current system state.

IV. PROPOSED SYSTEM

User to send commands to SaaS after SaaS processes the commands and creates logs for that, it will send back response. While user gets the response, the agent may make its own logs or just processes the response to user. However, how can we prove that the consumer had used the SaaS or the nonrepudiation of activity? The simplest answer is asking the SaaS CSP to provide the logs of the software or services traditionally. But in

cloud environment, we should not expect the CSPs to supply as much help and quick as the local servers can. It means that we should keep another log locally and synchronously, so we can use

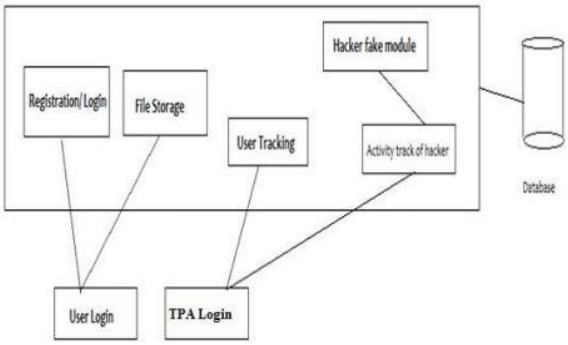

Figure1: Proposed System Architecture

it to check the activities on SaaS cloud while without the help of the CSPs. The content that would be recorded in the log files (the log files can be files or database) should be decided by the CSPs, but not the agent itself. That is to say the log files should be operated by a module created by the CSP. This is to make sure that the log files stored in local and in cloud are comparable. While the application on SaaS sends back the response, there will be a summary of the log record stored in SaaS, such as unique id and timestamp. The local log module will use that information on the log record locally. Additionally, for the consideration of protecting personal information, those files should be readable only to particular tools or software's that made by the CSP.

V. LOG BASED APPROACH FOR CLOUD FORENSICS

Digital forensic is a field to investigate the computer fault. Normal forensic investigation can use
for number of reasons. Criminal activity needs the investigation but as far as the digital forensic techniques are show it is capable of finding the hacker or the criminal user. Basically this user has its own identity like IP address, DNS name etc. Now days the internet is in access of normal user as well as attacker. Here the forensics investigator should be able to track an attacker on the Internet. The IP address and Domain name tracing is the first step to detect the doubtful user
Log file that have all the entry related to incoming user and leaving user. These file are generate by the process of mechanism. It can maintain by server machine, firewall, web servers, and routers etc. Generally the log files are in the text format can be read by notepad or simple text editor. Due to the plain text the size of log file will also reduces. In this model, consumer uses agent to send commands to SaaS and after SaaS processes the commands and creates logs for that, it will send back answer. While customer gets the answer, the mediator may make its own logs or just processes the answer to user. However, how can we prove that the customer had used the SaaS or the non repudiation of activity? The simplest answer is asking the SaaS CSP to provide the logs of the software or services traditionally[4]. But in cloud environment, we should not expect the CSPs to supply as much help and quick as the limited servers can. It means that we should keep another log locally and synchronously, so we can use it to check the activities on SaaS cloud while without the help of the CSPs. The content that would be recorded in the log files should be decided by the CSPs, but not the mediator itself. That is to say the log files should be operated by a module produced by the CSP. This is to make sure that the log files stored in local and in cloud are equivalent. While the application on SaaS sends back the answer, there will be a summary of the log record stored in SaaS, such as unique id and timestamp[2].
The local log module will use that information on the log record locally. In addition, for the concern of protecting personal information, those files should be readable only to particular tools or

software that made by the CSP. Illustrate the whole process of the communication concisely. Whilst there is another question that is how to guarantee the validity of them, if the log files are stored close by HASH code is known as the simplest kind of fingerprint for digital data. So we can use it to detected modification on the log files. Considering the growing speed of the log files in size, we can use an incremental HASH algorithm to get better the efficiency and reduce the time spending to verify. It will be very of use, because the investigators may be more interested in the recently events[5].

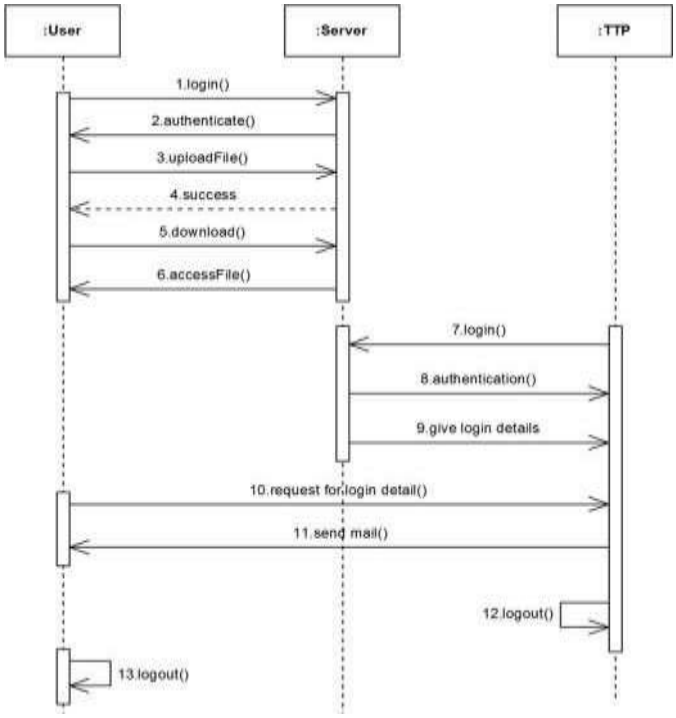

FIG 1. New Communication Model

1.Security

Encryption is a process used to protect information in transit and storage. It involves conversion of clear text data into cipher text, which cannot be read by unauthorized people For Encryption(uploading File) RSA is one of the first practicable public-key Cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977. A user of RSA creates and then publishes a public key based on the two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime numbers can possibly decode the message. The working of RSA is shown in figure 3. The RSA algorithm involves three steps: key generation, encryption and decryption.

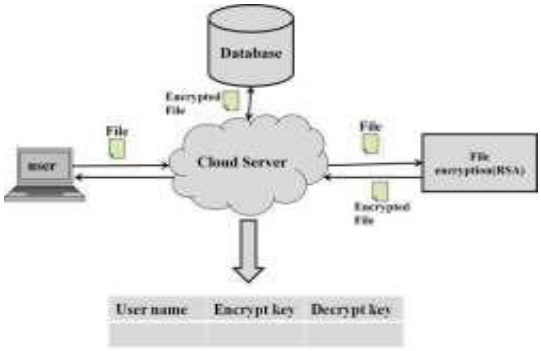

FIG 2. Encryption of File.

a) Key Generation Algorithm:
RSA public and private key pair can be generated by the following procedure. Choose two random prime numbers p and q such that the bit length of p is approximately equal to the bit length of q. The key set is generated by using the following algorithm:
1. Select two large prime numbers p and q such that p q.
2. Compute modulus n = p*q

3. Compute (n) such that (n) = (p–1)* (q–1).
4. Choose a random integer e satisfying 1<e < (n) and gcd (e, (n)) =1
5. Compute the integer d, such that e*d = 1 mod (n). (n, e) is the public key, and (n, d) is the private Key.
The RSA implementation is shown in figure

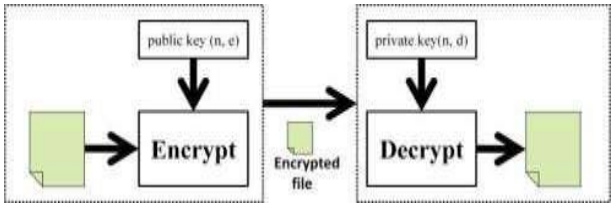

FIG 3. RSA implementation.

b)Encryption: Encryption refers to algorithmic schemes that encode plain text into non-readable form or cipher text, providing privacy.
c)Decryption: Decryption refers to algorithmic schemes that decode cipher text or non-readable text into readable form or pain text.
By using this model, we can obviously decrease the complexity of verifying if someone or some device has used the cloud services

V. CONCLUSION

From analysis part, we identify that cloud forensics is a cross-discipline between digital forensics and cloud computing. Various aspects of forensic in cloud computing in terms of security and privacy issues, conceptual and architectural, challenges and opportunity and the cloud forensic have been reviewed. Additionally, security and privacy in cloud forensics issues, most journals focus on the need for better understanding a probable risk involve if the breach of data in cloud computing happen and what the countermeasure need to be available for the ease of the forensic investigation need to be done. Thus it will lead to the involvement of the trusted third party, where most of the times can offer a more secured solution for the end users rather than the CSP. The log- based model can help to reduce the complexity of forensic for non repudiation of behaviors on cloud.

VI. ACKNOWLEDGMENT

We would like to acknowledge the guidance of Prof. Ajay. K. Gupta for her insightful support and inspiration throughout the various stages of this project. We sincerely appreciate the help and advice given by her which went a long way in helping us understanding the key concepts of this project.

REFERENCES

[1]Technical Issues of Forensic Investigations in Cloud Computing Environments. Prof. Birk, D.; Wegener, C. 6th International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE)

[2]Cybercrime forensic system in cloud computing, Image Analysis and Signal Processing (IASP) Prof.Cheng Yan, pages: 612-615, 2011.Stephen Biggs, Stilianos Vidalis.

[3] Birk, D.; Wegener, C. Technical Issues of Forensic Investigations in Cloud Computing Environments. 6th International Workshop on Systematic Approaches to Digital Forensic computing market forecast

[4]Engineering(SADFEAhmed,S.Raja,M.Y.A. Tackling cloud Computing: The impact ondigital forensic security issues and forensics model. High-investigations. International Conference for Internet Technology and Secured Transactions, Capacity Optical Networks and Enabling Technologies (HONET), 2010.