A Log Based Approach to Make Digital Forensics Easier on Cloud Computing

Jadhav Avinash S.[1] Khaire Pranjal B.[2] Borse Madhuri N.[3] Prof. Chandgude A. S.[4]
[1,2,3]B.E Student [4]Professor
[1,2,3,4]Department of Computer Engineering
[1,2,3,4]SND COE & RC Yeola, Maharashtra, India

Abstract— Cloud computing is getting huge attention from the IT industry recently. Almost all the top most companies of the IT sector showing their interest and efforts on cloud computing and release services about cloud computing in succession. We should further improve the cloud computing not only at the feature of precaution, but also at the feature of dealing with the security events to defend it from the crime pursuit. In this system we provide cloud security in this system Using Intelligent encryption technology so any user can store his/her file securely .In this system we also tracking user log such as login time, Log out time, IP address etc. We also implementing fake Module for hacker. Using this forensic-friendly system model we can quickly gather information from cloud computing for some kinds of forensic purpose. And this perspective decreases the complexity of those kinds of forensics. log is a regular or systematic record of actions that object has taken or statuses that object have been. It is the most common component that be used in digital forensic.

Keywords: Digital Forensic, Log, Cloud-Computing, Security

I. INTRODUCTION

Cloud computing is one of the leading technology in recent years. Many companies fascinated about the cloud computing because of these main characteristics like low cost in using, independence of location, performance and reliability and etc. Because of these benefits, all companies no need to waste money on hardware and they can setup their business easily, Cloud services provide three major delivery models those are PaaS i.e. Platform as a Service, IaaS i.e. Infrastructure as a Service and SaaS i.e. Software as a Service. We can say in normal usage, the term quota; the cloud quota; is essentially a trope for the Internet. Marketers have made popularized the phrase quota; in the cloud quota; to says software, platforms and infrastructure that are sold quotas a service quota; to the end users, i.e. remotely through the Internet. Typically, the vendor has actual energy consuming servers which host products and services from a remote location, so end-users don't have to bother about server maintenance etc.; they can simply log on to the network without installing anything they can access services. The major models of cloud computing service are known as, platform as a service, Software as a Service and Infrastructure as, a service. Google, Amazon, IBM, Oracle Cloud, Rackspace, Salesforce, Zoho and Microsoft. Cloud security should contain two categories. One is how to protect cloud and other one is applications running inside from attack. And then how to deal with the happened security events. Precaution is the major concern on cloud security, but we should know that no wall is wall in the world. Criminal always can discover any way to overcome the security threats to get succeed in their goals illegally. In the digital world, the security department had started a new field of battle with criminals.

II. LITERATURE SURVEY

A. Cloud Security Architecture Based on User Authentication and Symmetric Key Cryptographic Techniques:

Cloud computing is having the capacity to dispose of the prerequisites for setting up high cost computing framework and promises to provide flexible architecture which is accessible from anywhere. The data in the cloud computing resides over an arrangement network resources which enables position of the requirements for setting up costly data centers framework and information to be acquired via virtual machines and these serves might be arranged in any part of the world. The cloud computing environment is adopted by large number of organizations so the rapid minimum effort. The advantages of distributed computing incorporate diminishing the equipment and support cost, accessibility around globe, adaptability and to a great degree mechanized process. It conveys unfathomable advantages to both Individuals and ventures by decreasing the requirement for client association by concealing specialized points of interest, for example updates, licenses and support from its clients. Cloud can like wises provide improved safety over single server arrangements subsequently cloud totals resources and permits licensed security individual while as the typical organizations are restricted with system and network admin who won't be well learned about cyber security issues. With rising concerns regarding the cloud computing and security of data the prominent security algorithms especially. symmetric algorithms could be widely used in cloud application services which involve encryption techniques. Cryptography is used in hiding information from intruders and storing it confidentially so that only those users and are able to whom it is intended for and communication this information securely. The use security algorithms minimize security concerns with the help of cryptographic and authenticating techniques, cryptography is the process of crafting message securely altering the data to be sent with encrypting the plain text by taking user data and then executing the reverse process called as decryption which is returning back to original text. The cryptography can resolve the problems in cloud computing regarding network data and server security.

B. Cost Effective Authentic and Anonymous Data Sharing with Forward Security

The popularity and widespread use of CLOUD" have brought great convenience for data sharing and collection. Not only can individuals acquire useful data more easily, sharing data with others can provide a number of benefits to our society as

well. As a representative example, consumers in Smart Grid can obtain their energy usage data in a fine-grained manner and are encouraged to share their personal energy usage data with others, e.g., by uploading the data to a third party platform such as Microsoft Hohm . From the collected data a statistical report is created, and one can compare their energy consumption with others (e.g., from the same block). This ability to access, analyze, and respond to much more precise and detailed data from all levels of the electric grid is critical to efficient energy usage. Due to its openness, data sharing is always deployed in a hostile environment and vulnerable to a number of security threats. Taking energy usage data sharing in Smart Grid as an example, there are several security goals a practical system must meet, including:

Data Authenticity: In the situation of Smart Grid, the statistic energy usage data would be misleading if it is forged by adversaries. While this issue alone can be solved using well established cryptographic tools (e.g., message authentication code or digital signatures), one may encounter additional difficulties when other issues are taken into account, such as anonymity and efficiency; Anonymity: Energy usage data contains vast information of consumers, from which one can extract the number of persons in the home, the types of electric utilities used in a specific time period, etc. Thus, it is critical to protect the anonymity of consumers in such applications, and any failures to do so may lead to the reluctance from the consumers to share data with others searches over the encrypted cloud data.

C. Technical Issues of Forensic Investigations in Cloud Computing Environments:

In this paper is based on Cloud Computing is arguably one of the most discussed information technologies today. It presents many promising technological and economic opportunities. However, many customers remain reluctant to move their business IT infrastructure completely to the cloud. One of their main concerns is Cloud Security and the threat of the unknown. Cloud Service Providers (CSP) encourage this perception by not letting their customers see what is behind their virtual curtain. A seldom discussed, but in this regard highly relevant open issue is the ability to perform digital investigations. This continues to fuel insecurity on the sides of both providers and customers. Cloud Forensics constitutes a new and disruptive challenge for investigators. Due to the decentralized nature of data processing in the cloud, traditional approaches to evidence collection and recovery are no longer practical. This paper focuses on the technical aspects of digital forensics in distributed cloud environments. We contribute by assessing whether it is possible for the customer of cloud computing services to perform a traditional digital investigation from a technical point of view. Furthermore we discuss possible solutions and possible new methodologies helping customers to perform such investigations. Although the cloud might appear attractive to small as well as to large companies, it does not come along without its own unique problems. Outsourcing sensitive corporate data into the cloud raises concerns regarding the privacy and security of data. Security policies, companies main pillar concerning security, cannot be easily deployed into distributed, virtualized cloud environments. This situation is further complicated by the unknown physical location of the companies assets. Normally, if a security incident occurs, the corporate security team wants to be able to perform their own investigation without dependency on third parties. In the cloud, this is not possible anymore: The CSP obtains all the power over the environment and thus controls the sources of evidence. In the best case, a trusted third party acts as a trustee and guarantees for the trustworthiness of the CSP

D. Tackling Cloud Security Issues and Forensics Model:

Cloud computing is getting increased attention of the information and communication technologies (ICT) industry recently. The cloud service providers foresee it as a source of promising financial gains, the clients find it a convenient solution where the enterprises. may get started on their computing activities without investing on the in-house facilities of hardware and software. They can outsource the computing and archiving activities to the cloud service providers (CSP) though Internet.

III. PROPOSED SYSTEM

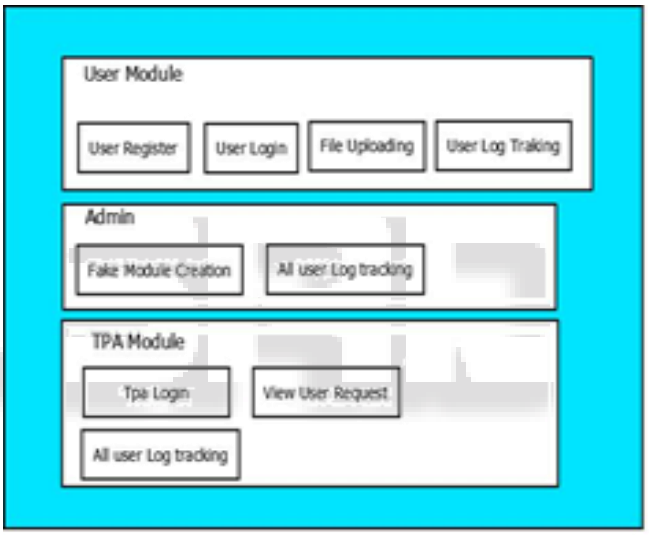

Fig. 1: Proposed System

We thus propose the large number of data users and documents in cloud, it is crucial for the search service. So we provide cloud Security to Data. In this system we cover technical aspects of digital forensics in distributed cloud environments.

A. Advantages of Proposed System:

1) The ability to reduce or even eliminate sampling risk. This is the biggest advantage of forensic accountants over the external auditors.
2) The comparison of relevant types of data from different systems or sources to show a more complete picture.
3) The identifying trends of which company personnel, consultants and forensic accountants were unaware
4) The testing for effectiveness of the control environment and policies in place by identifying attributes that violate rules.
5) The ability to easily trend relevant data over periods of time; fluctuations in trending lines can be analyzed further for false positives and potential risk factors.

B. Module:

There are Four Module in System:

1) User Login
2) TPA Login
3) Hacker
4) Admin

IV. CONCLUSION

The cloud computing is a new platform which is a potent solution for a number of applications in ICT industry. Some of these areas include large data archives, ultra /super computer speeds of computing engine configurable on demand with pay as you go feature. The business enterprise structures are going to experience a significant new dimension where the physical office environments and in house IT infrastructure will not necessarily be required. In such solutions the data within the enterprise is maintained in the local or enterprise cloud which is extended to the cloud domain hosted by a service provider. The cloud computing models have to win the trust of clients through acceptable security procedures. The client may choose for levels of security with a corresponding service cost structure. The security control measures offered by the CSPs at present are not sufficient to address the concerns of business and research communities.

V. SCREENSHOTS

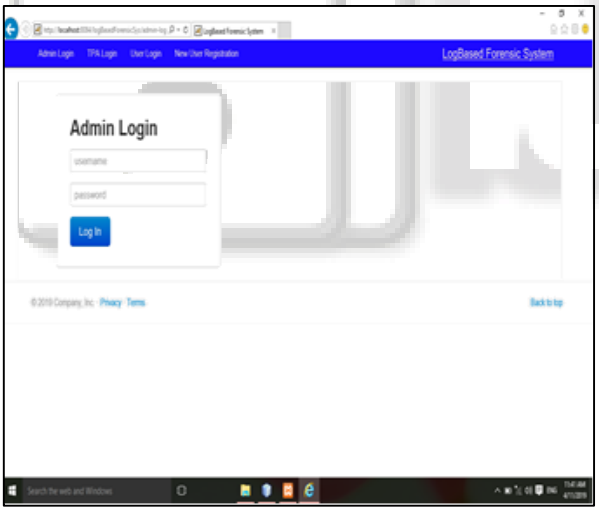

Fig. 2: Admin Login

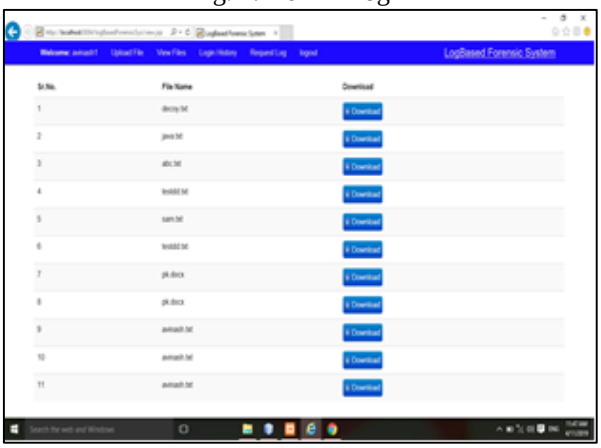

Fig. 3: All Files

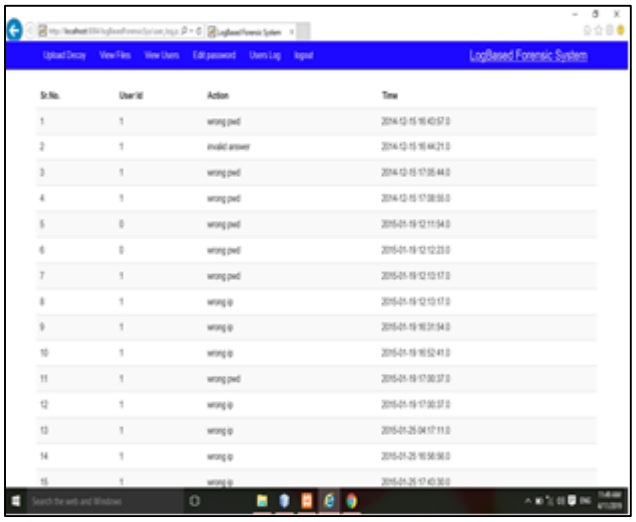

Fig. 4: User Logs

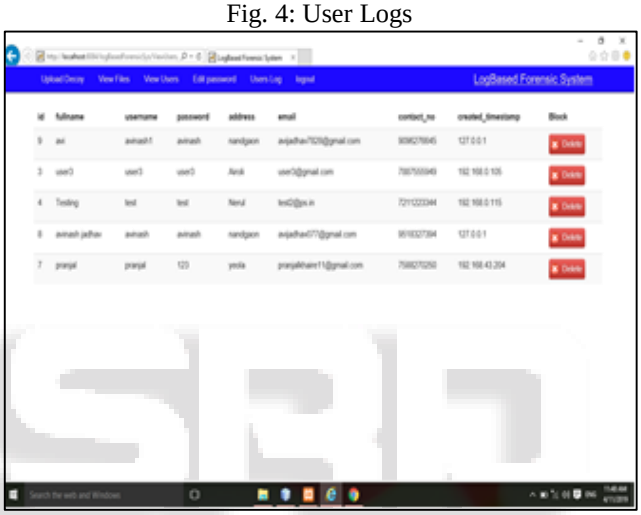

Fig. 5: All Users

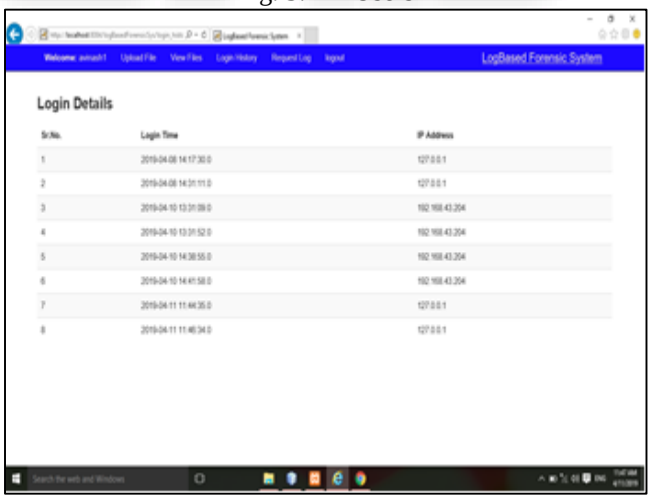

Fig. 6: Login History

REFERENCES

[1] d. boneh, x. boyen, and h. shacham, "'short group signaturess",in crypto 2004,volume 3152 of lecture notes in computer science, pages 4155. springer, 2017.
[2] N. De Silva, J. S. Goonetillake, G. N. Wikramana yake,
[3] Hengshu Zhu, Enhong Chen, Hui Xiong, Huanhuan Cao, and Jilei Tian"Mobile App Classification with Enriched

Contextual Information IEEE Transactions on mobile computing (Volume:13 , Issue: 07),7 July 2016.

[4] D. Barrera, H.G. Kayacik, P.C. van Oorschot, and A. Somayaji "A Methodology for Empirical Analysis of Permission-Based Security Models and Its Application to Android, Proc. 17th ACM Conf. Computer and Comm. Security, pp. 73-84, 2015.

[5] X.-H. Phan et al."A hidden topic-based framework toward building applications with short web documents, IEEE Trans. Knowl. Data Eng., vol. 23, no. 7, pp. 961976, Jul. 2014.

[6] M. Sahami and T. D. Heilman, "A web-based kernel function for mea-suring the similarity of short text snippets, in Proc. WWW, Edinburgh, U.K., 2006, pp. 377386.

[7] H. Ma, H. Cao, Q. Yang, E. Chen, and J. Tian "A habit mining approach for discovering similar mobile users, in Proc. WWW, Lyon, France, 2012, pp. 231240.

[8] W. Enck, P. Gilbert, B. Chun, L.P. Cox, J. Jung, P. McDaniel, and A.N Sheth "TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones, Proc. Ninth USENIX Conf. Operating Systems Design and Implementation, article 1-6, 2010.

