ISSN: 2321-7782 (Online)
Volume 3, Issue 9, September 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Design and Development of System for detection of security Breach in Cloud Environment

Sulabha Patil[1]
Assistant Professor, M.Tech (CSE)
TGPCET
Nagpur, India

Uzma Ali[2]
Student,M.Tech(CSE)
TGPCET
Nagpur, India

Dr. R. V. Dharaskar[3]
Ex-Director
Disha Group of Institution
Nagpur, India

Abstract: ***Cloud Computing has brought an incredible change in operations of the IT industries. The cloud computing has benefited the IT industries with less infrastructure investment and maintenance. As cloud provides services like Infrastructure-as-service (IaaS), Platform-as-Service (PaaS) and Software-as-service (SaaS) to its clients, it is essential that it also ensures data security to its clients. Security is an essential service to be provided exclusively in public cloud and hybrid cloud environment where in the data can be easily hacked or tampered. Nowadays, digital storage of computer data is moving toward cloud computing which is a set of infrastructure provides data storage for organizations and individuals. Due to this large scale, in case an attack occurs in the network of a cloud it would be a big challenge to investigate the cloud. This paper aims to implement the development of system for detection of security breach in cloud environment by introducing the non-repudiation in MVC Music Library application.***

Keywords: Cloud Computing, Security, Digital Forensic, Virtualization, Non-repudiation

I. INTRODUCTION

Cloud computing which is also known as 'Internet computing' generally is seen as collection of clouds on the web. It provides technology enabled services to the people and organizations by utilizing the internet. People can just access to the web anywhere and at any time without to think about the physical 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 convenience, flexibility and more performance on demand network access which is consisting of five essential characteristics, three service models and four deployment models. These five essential characteristics of cloud computing are on-demand selfservice, broad network access, rapid elasticity, resource pooling and measured service [6].

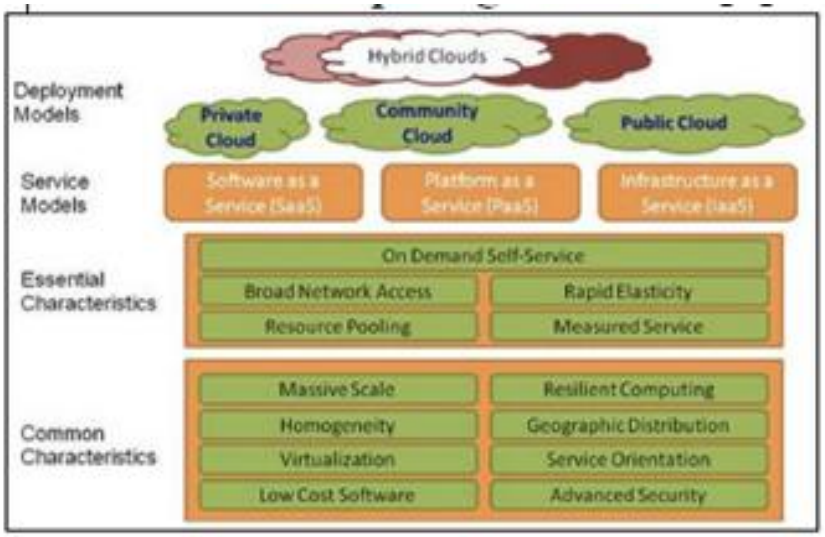


Fig. 1: The NIST Cloud Definition Framework

Cloud computing composed of three service models that are Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS) and Cloud Infrastructure as a Service (IaaS). SaaS is where the application is hosted and delivered online through a web browser; PaaS is where the cloud provides the software platform for systems while IaaS is a set of virtualized computing resources. The four cloud deployment models are the Public Clouds, Community Clouds, Private Cloud and Hybrid Cloud. Fig.1 above is the overall picture of the cloud computing definition given by NIST. Based on the standard definition given by the NIST, cloud computing aim to make a better use of distributed resources and combine them to achieve higher throughput as well as to be able to solve large scale computation problems [6].

Digital forensics is the process of preserving, collecting, confirming, identifying, analyzing, recording, and presenting crime scene information. Wolfe defines digital forensics as “A methodical series of techniques and procedures for gathering evidence, from computing equipment and various storage devices and digital media that can be presented in a court of law in a coherent and meaningful format". According to a definition by NIST, computer forensics is an applied science to identify an incident, collection, examination, and analysis of evidence data. While doing so, maintaining the integrity of the information and strict chain of custody for the data is mandatory. Several other researchers define computer forensics as the procedure of examining computer system to determine potential legal evidence [10].

Cloud forensics can be defined as applying computer forensics procedures in a cloud computing environment. As cloud computing is based on extensive network access, and as network forensics handles forensic investigation in private and public network, Ruan et al. defined cloud forensics as a subset of network forensics. They also identified three dimensions in cloud forensics – technical, organizational, and legal. Cloud forensics procedures will vary according to the service and deployment model of cloud computing. For Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS), we have very limited control over process or network monitoring. Whereas, we can gain more control in Infrastructure-as-a-Service (IaaS) and can deploy some forensic friendly logging mechanism. The first three steps of computer forensics, identification, collection, and organization of evidence will vary for different service and deployment model. For example, the evidence collection procedure of SaaS and IaaS will not be same. For SaaS, we solely depend on the CSP to get the application log, while in IaaS, we can acquire the virtual machine image from the customer and can enter into examination and analysis phase. On the other hand, in the private deployment model, we have physical access to the digital evidence, but we merely can get physical access to public deployment model [10].

II. Proposed Methodology

Security is the important aspect in Cloud computing. Various attacks such as DoS, DDoS, sniffer attack, spoofing, phishing, Non-repudiation and so on are there in network. To detect non-repudiation attack in cloud environment, we proposed

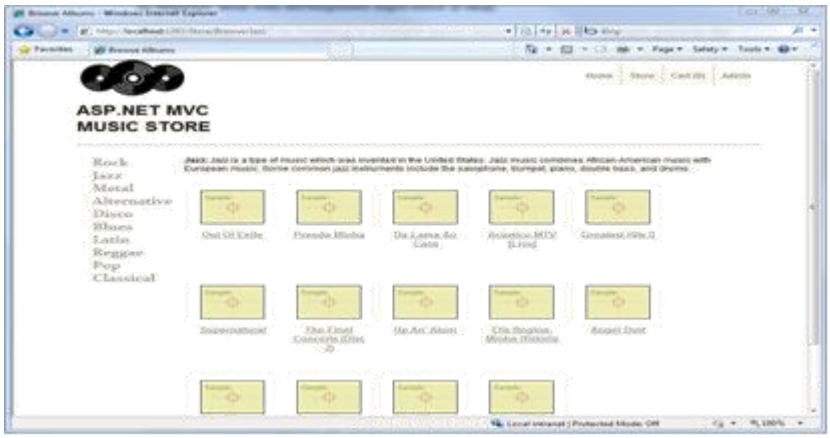
the simple system such as music library for detecting the security breach in cloud environment by capturing the conventional and forensic data.

The application of music library is developed by using the .net platform is hosted in the cloud environment and the non-repudiation is detected by capturing the forensic data such as longitudinal and latitudinal information even the conventional information.

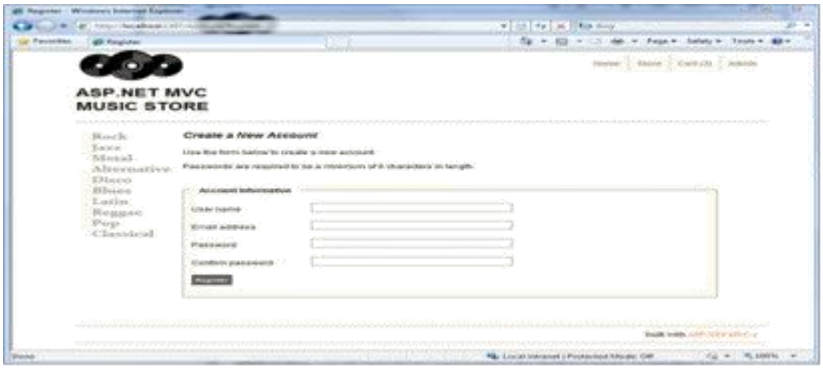
III. Implementation of Proposed Methodology

The application is a simple music store. There are three main parts to the application: shopping, checkout, and administration.

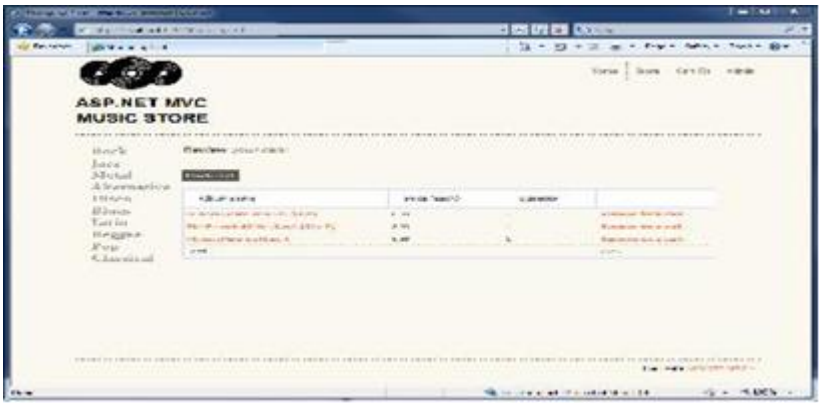
Visitors can browse Albums by Genre:



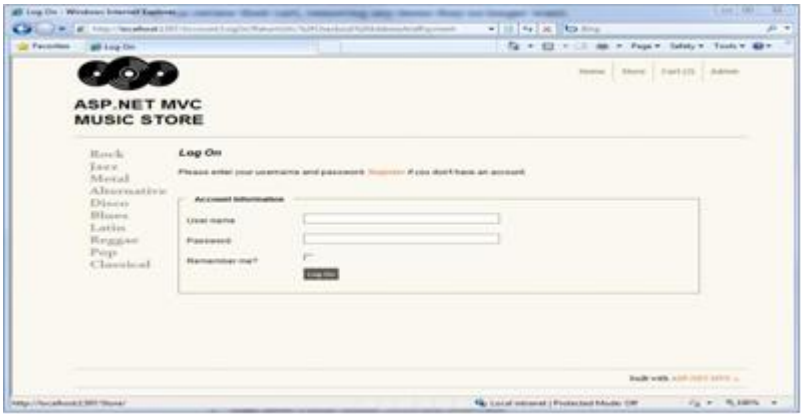
They can view a single album and add it to their cart:



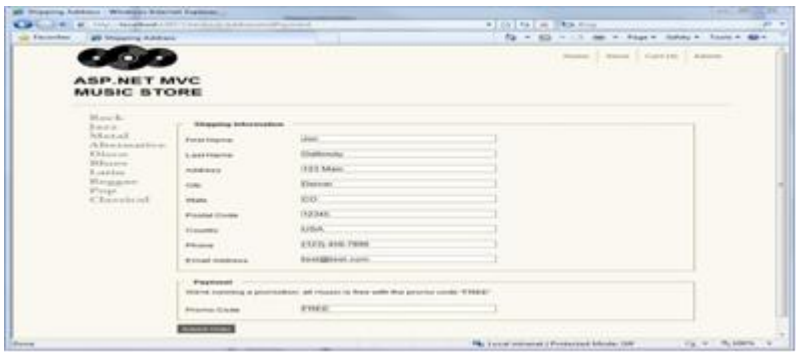
They can review their cart, removing any items they no longer want:



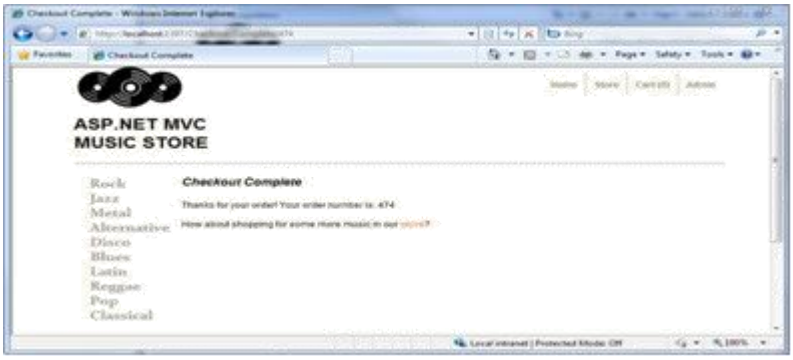
Proceeding to Checkout will prompt them to login or register for a user account.



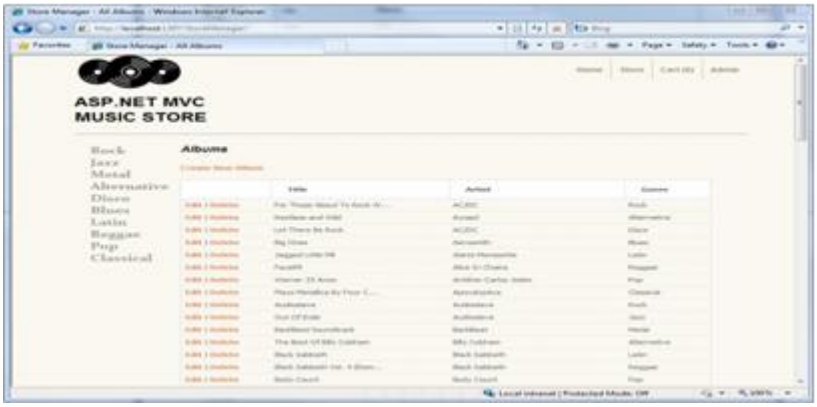
After creating an account, they can complete the order by filling out shipping and payment information.



After ordering, they see a simple confirmation screen:



The Administration page shows a list of albums from which Administrators can Create, Edit, and Delete albums:



IV. RESULT AND ANALYSIS

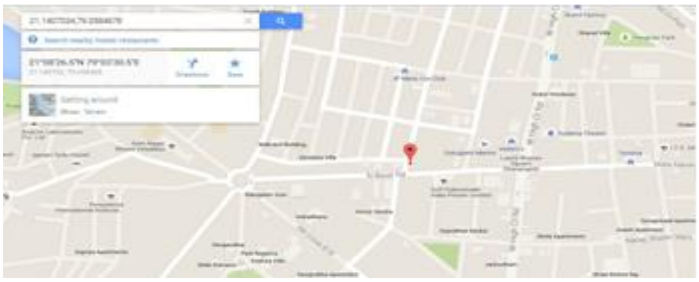
Cloud Computing has been considered as the future of IT that leads to novel computing models. However, security has been one of the major concerns that prevent commercial applications from being accepted widely. Here we are introducing non-repudiation in system and reporting that by capturing the LAN ip, machine name, user name, public ip, time and most probably the geographical location of the user.

Capture Admin home screen:

Capture transaction log of users as shown in below screen:

The data we are fetching and storing in database .It consist of current data as well as last transaction data which is stored in cookie shown in the given screen as follows:

Even we are showing the location on google map .The two locations on google map are as follows: Current location:



Last transaction location on Google map as follows:

V. Conclusion and Suggested Future Work

Cloud computing is a rapidly emerged technology and it is a widely accepted computing paradigm all around the world by its advantages on quick deployment, cost efficiency (on setting up and improvement), large storage space, and easy access to system anytime and anywhere. Apart from these advantages it has some disadvantages on security and privacy concerns, which are seen as the primary obstacles to wide adoption. At the same time, because of the distributed nature of the system, there is a risk of security attacks on services and resources in cloud computing. These attacks can be both outside and inside the cloud provider's network. We have studied one type of attack detection in cloud environment i.e. Non-repudiation. Designed the system of Music library and studied the Non-repudiation in cloud environment.

The future work is to study the experimental performance of various attacks such as phishing, spoofing,DoS, DDoS, man-in-the-middle, sniffer and its detection in cloud environment by capturing forensic and conventional data by developing the various application in cloud environment.

References

1. Le Xu, Dijiang Huang, Wei-Tek Tsai," Cloud-Based Virtual Laboratory for Network Security Education" IEEE Transactions on Education, Vol. 57, No. 3, August 2014.
2. Zahid Anwar and Asad Waqar Malik," Can a DDoS Attack Meltdown My Data Center? A Simulation Study and Defence Strategies" IEEE Communications Letters, Vol. 18, No. 7, July 2014.
3. Deoyani Shirkhedkar, Sulabha Patil," Design of digital forensic technique for cloud computing" Volume 2, Issue 6, June 2014 International Journal of Advance Research in Computer Science and Management Studies.
4. Chun-Jen Chung, Tianyi Xing, And Dijiang Huang," NICE: Network Intrusion Detection And Countermeasure Selection In Virtual Network Systems" IEEE Transactions On Dependable And Secure Computing, Vol. 10, No. 4, July/August 2013.

5. Zhifeng Xiao and Yang Xiao," Security and Privacy in Cloud Computing" IEEE Communications Surveys & Tutorials, Vol. 15, No. 2, Second Quarter 2013.

6. Farid Daryabar, Ali Dehghantanha, Nur Izura Udzir, Nor Fazlida binti Mohd Sani, Solahuddin bin Shamsuddin, Farhood Norouzizadeh," A Survey About Impacts of Cloud Computing on Digital Forensics" International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2(2): 77-94The Society of Digital Information and Wireless Communications, 2013 (ISSN: 2305-0012).

7. Zhen Chen, Fuye Han, Junwei Cao, Xin Jiang, and Shuo Chen," Cloud Computing-Based Forensic Analysis for Collaborative Network Security Management System" TSINGHUA SCIENCE AND TECHNOLOGY ISSNl l1007-0214l l05/12l lpp40-50 Volume 18, Number 1, February 2013.

8. Khaled Salah, Jose M. Alcaraz Calero, Sherali Zeadally, Sameera Al-Mulla and Mohammed Alzaabi January/February. 2013 Copublished by the IEEE Computer and Reliability Societies 1540-7993/13/$31.00©2013IEEE

9. U. Oktay and O.K. Sahingoz," Attack Types and Intrusion Detection Systems in Cloud Computing", 20-21 September /Eylül 2013 | Ankara / TURKEY / Proceedings/Bildiriler Kitabı pp 71-76 2013.

10. Shams Zawoad and Ragib Hasan, "Digital Forensic in the Cloud", CrossTalk—September/October 2013 pp17-20, 2013.

11. Patrick Honer," Cloud Computing Security Requirements and Solutions: a Systematic Literature Review" University of Twente, 2013 - referaat.cs.utwente.nl.

12. H. Guo, T. Shang and B. Jin, "Forensic Investigations in Cloud Environments,"International Conference on Computer Science and Information Processing (CSIP), pp 248-251, August 2012.

13. J.Srinivas, K.Venkata Subba Reddy, Dr.A.Moiz Qyser,"Cloud Computing Basics"International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 5, July 2012.

14. Ashalatha R," A Survey On Security As A Challenge In Cloud Computing" ISSN No: 2250-3536 Volume 2, Issue 4, July 2012.

15. Abdul Wahid Khan, Siffat Ullah Khan, Muhammad Ilyas and Muhammad Ilyas Azeem,"A Literature Survey on Data Privacy/ Protection Issues and Challenges in Cloud Computing" IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661 Volume 1, Issue 3 (May-June 2012), PP 28-36.

16. Keyun Ruan, Prof.Joe Carthy, Prof.Tahar Kechadi, Ibrahim Baggili (PhD)," Survey on Cloud Forensics and Critical Criteria for Cloud Forensic Capability: A Preliminary Analysis"Jounal of Network Forensics vol.3, Issue 2011.

17. Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy, "Cloud Computing: Security Issues and Research Challenges", International Journal of Computer Science and Information Technology & Security (IJCSITS), Vol. 1, No. 2, December 2011.

18. B. Grobauer, T. Walloschek, and E. Stocker, "Understanding Cloud Computing Vulnerabilities," Security & Privacy, IEEE, vol. 9, no.2, pp. 50-57, 2011.

19. George Grispos Tim Storer William Bradley Glisson" Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics".

20. Dominik Birk, Christoph Wegener," Technical Issues of Forensic Investigations in Cloud Computing Environments".

21. Farzad Sabahi, "Secure Virtualization for Cloud Environment Using Hypervisor-based Technology", International Journal of Machine Learning and Computing, Vol. 2, No. 1, February 2012

22. Debojyoti Sengupta," A Survey on Security of Hypervisorbased Virtualization System in Cloud Computing"

23. Jakub Szefer, Ruby B. Lee," Architectural Support for Hypervisor-Secure Virtualization", International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS), March 2012.

24. Diego Perez-Botero, Jakub Szefer and Ruby B. Lee," Characterizing Hypervisor Vulnerabilities in Cloud Computing Servers", Workshop on Security in Cloud Computing (SCC), May 2013

25. Naresh Kumar, Shalini Sharma," Study of Intrusion Detection System for DDoS Attacks in Cloud Computing", 978-1-4673-5999-3/13 ©2013 IEEE

26. A.M. Lonea, D.E. Popescu, H. Tianfield," Detecting DDoS Attacks in Cloud Computing Environment", INT J COMPUT COMMUN, ISSN 1841-9836 ,8(1):70-78, February, 2013.

AUTHOR(S) PROFILE

Prof. Sulabha Patil, working as Asst. Professor at TGPCET, Nagpur, pursuing Ph.D. in Computer Science and Engineering **.**She received the M.E. degree in Wireless communication and computing. She had completed MCA and MBA. She had graduate degree of B.Tech in applied electronics. Her research area is cloud computing and networking.

Uzma Ali, Student of M.Tech (Computer Science and Engineering) at TGPCET, Nagpur. She received the degree of MCA in year 2009.She had completed her graduation in B.Sc. Computer Science. Her research area is Cloud computing, data mining and networking.

Dr. R. V. Dharaskar, Former director of Disha Education society, Raipur (CG). He is Former Director, MPGI Integrated Campus Group of Institutes, Nanded, MS and even Former Prof. & Head, Department of CSE, GHRCE (TEQIP funded Autonomous Institute), Nagpur, MS. His Series of Books, published by Shroff Publication (SPD).

