A SURVEY ON FORENSICS AND INVESTIGATION IN CLOUD ERA

[1]A Kavitha, [2]P Sudheer Babu, [3]K Navatha, [4]E Soumya

[1,2,3]Assistant Professor, [4]Associate Professor
[1]Computer Science and Technology,
[1,2,4]St.Martin's Engineering College, Hyderabad, India,
[3]Sreyas Institute of Engineering and Technology, Hyderabad, India

Abstract: **Cloud computing is advancing electronic innovation. Which give different support of physical IT foundation which is overseen and facilitated by third party Highlights because of which cloud discover its application in E-learning, cloud based ERP and E-governance are adaptability, accessibility, versatility, productivity and unwavering quality. As huge number of registering innovation is included in it is a question of security issues. This paper describes the forensics in the cloud challenges and investigation.**

Keywords **- Cloud Computing, Cloud Computing Forensics**

1. INTRODUCTION

Distributed computing has upset the advanced world. It has totally changed the substance of physical PC, programming utilized and database stockpiling. As per the official NIST definition, "cloud registering is a model for empowering pervasive, helpful, on-request organize access to a common pool of configurable processing assets (e.g., systems, servers, stockpiling, applications and administrations) that can be quickly provisioned and discharged with negligible administration exertion or specialist organization interaction[1]. Another definition by Open Cloud Proclamation Consortium characterizes the key parts of distributed computing as: "the capacity to scale and arrangement figuring power powerfully in a cost-effective manner and the capacity of the purchaser (end client, association, or IT staff) to capitalize on that power without having to deal with the basic multifaceted nature of the innovation. (The Open Cloud Manifesto Consortium, 2009)"[2] With this we presume that this routine with regards to shared information assets has made distributed computing to go about as a impetus for universal processing. It has change the customary approach of IT world. The highlights of distributed computing that have changed the substance of physical registering and have asked conventional merchants to move to the cloud innovation have been recorded in this segment.

- Resource pooling
- On request benefit
- Scalability
- Virtualization
- Reliability
- Maintainability
- High execution
- Customizable
- Location free
- Multitenancy
- Efficient asset usage
- Cost pay-as-utilize

1.1. Why Cloud Computing

In this area, we have investigated what is making cloud fast advances. Lessened work cost the examination demonstrates that cloud diminish work cost by half in observing and support, which bring
Critical benefit to business.[8] Upgrades usage rate Cloud upgrade the usage rate of different segment through virtualization (para virtualization, incomplete virtualization or full virtualization).

Lessens consummation time Area free accessibility of assets lessens consummation time from weeks to minutes Lessened task cost The Saas in view of pay as you go display altogether cuts the venture cost and lessens the cost of buying programming permit and programming.

1.2 Cloud Computing Models

To additionally sophisticate the approach of registering, cloud has distinctive models as indicated by the cloud condition, proprietorship, size and access required by the customer.
Open cloud: application and capacity for open over the web.
Example Amazon EC2, IBM's Blue Cloud and Google Application.

Private cloud: service and infrastructure are dedicated to particular organization. It is more secure and expensive than public cloud.
Hybrid cloud: combination of both public and private cloud. Use of private cloud in public cloud with set boundaries.
Community cloud: Organization belonging to same community share computing infrastructure.

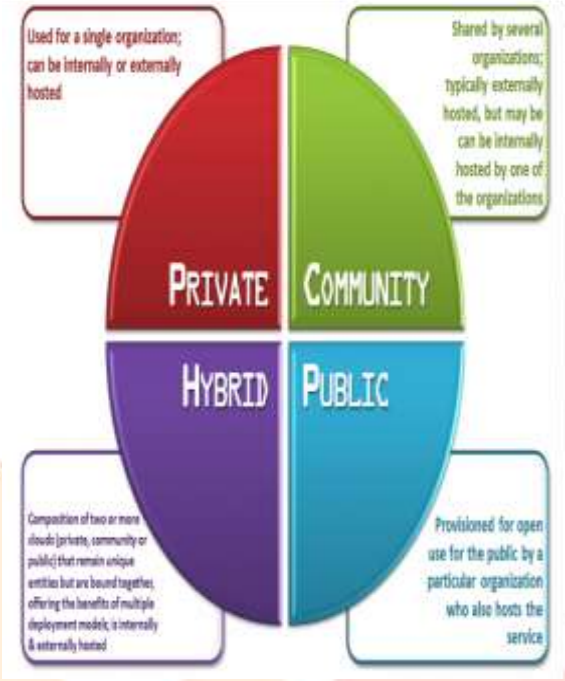

Figure 1: Cloud Models

2. CLOUD SERVICE MODELS

Saas Software as a service referred as "on demand service" in which organization need not to install and run application on their computer, third party provider makes the application available to customer by hosting over the internet.

Paas Set of tools and services designed to make coding and deploying those applications quickly and efficiently.

Iaas Is the hardware and software that powers server, storage, network, operating system? It basically provides the infrastructure requirement of the organization.

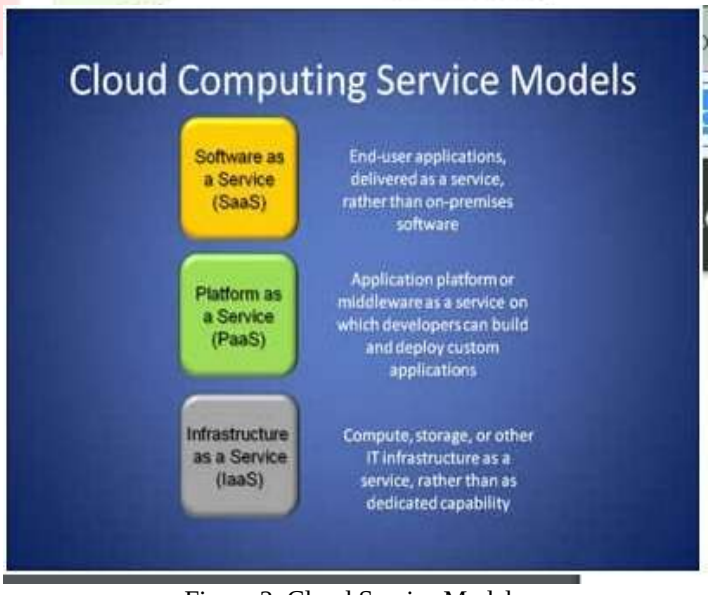

Figure 2: Cloud Service Models

3. PROPOSED WORK

3.1 Cloud Forensics in Cloud Era

Cloud forensics is a cross discipline of cloud computing and digital forensics. Cloud computing is a shared collection of configurable networked resources (e.g., networks, servers, storage, applications and services) that can be reconfigured quickly with minimal effort [12]. Digital forensics is the application of computer science principles to recover electronic evidence for presentation in a court of law [10].

Cloud forensics is a subset of network forensics. Network forensics deals with forensic investigations of networks. Cloud computing is based on broad network access. Therefore, cloud forensics follows the main phases of network forensics with techniques tailored to cloud computing environments.

Cloud computing is an evolving paradigm with complex aspects. Its essential characteristics have dramatically reduced IT costs, contributing to the rapid adoption of cloud computing by business and government [5].

To ensure service availability and cost-effectiveness, CSPs maintain data centers around the world. Data stored in one data center is replicated at multiple locations to ensure abundance and reduce the risk of failure. Also, the segregation of duties between CSPs and customers with regard to forensic responsibilities differ according to the service models being used. Likewise, the interactions between multiple tenants that share the same cloud resources differ according to the deployment model being employed.

Multiple jurisdictions and multi-tenancy are the default settings for cloud forensics, which create additional legal challenges. Sophisticated interactions between CSPs and customers, resource sharing by multiple tenants and collaboration between international law enforcement agencies are required in most cloud forensic investigations.

In order to analyze the domain of cloud forensics more comprehensively, and to emphasize the fact that cloud forensics is a multi-dimensional issue instead of merely a technical issue, we discuss the technical, organizational and legal dimensions of cloud forensics.

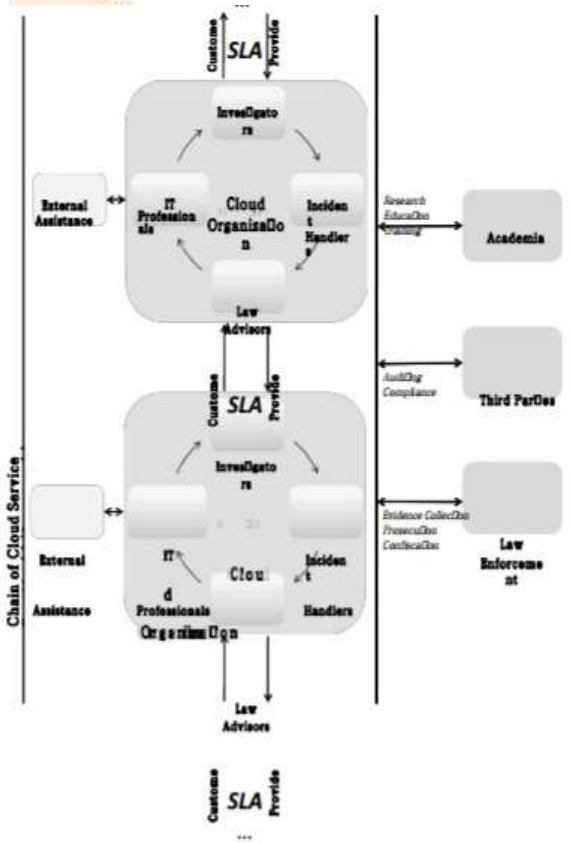

Figure 3: Cloud Computing forensic entities

4. CONCLUSION

Cloud computing is pushing the boondocks of computerized crime scene investigation.TheCloud compounds numerous innovative, authoritative and lawful difficulties. A few of these difficulties, for example, information replication, area straightforwardness and multi-occupancy, are novel to cloud criminology. In any case, cloud criminology brings one of a kind open doors that can fundamentally the adequacy and speed of criminological examinations. These security issues lead to various cloud breach which paves the way for many cybercrimes. In this section, we discuss about the challenges faced during cloud forensic investigation. The Cloud face of IT industry in terms of application, concept, cost, security and availability is undoubtedly commendable. Various service model and types of cloud makes cloud computing effective, categorical service, geological load balancing, improved performance and service. Cloud application reduces the cost, enhances business outcomes and significantly improves performance. Cloud Forensic is challenging and is pushing the boundaries of digital forensics. Cloud forensics brings many technological, legal, geographical and organizational challenges.

REFERENCES

[1] NIST Cloud Computing 11 Forensic Science Challenges, Draft NISTIR

[2] Quoted under report, "The Open Cloud Manifesto Consortium: A call to action for the worldwide cloud community", Draft 1.0.7, 2008

[3] Nitin Kumar, Shrawan Kumar Kushwaha and Asim Kumar, "Cloud Computing Services and its Application" ISSN 2231-1297, Volume 4, Number 1 (2014)

[4] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez, "An analysis of security issues for cloud computing", Journal of Internet Services and Applications 2013

[5] Quoted under cloud ERP service provider, http://www.enterpriseappstoday.com/erp/11- cloud-erp-software-options-1.html

[6] Jon Brodkin "Gartner: Seven cloud-computing security risks Data integrity, recovery, privacy and regulatory compliance are key issues to consider", July 02, 2008

[7] 8006 Ahmed E. Youseef "Exploring cloud computing services and applications" vol. 3 no. 6 July 2012.

[8] H. Guo et al. "Forensic investigations in cloud environments", in Computer Science and Information Processing (CSIP), 2012 International Conference on. IEEE, 2012.

[9] Dominik Birk, "Technical Challenges of Forensic Investigations in Cloud Computing Environments, in Workshop on Cryptography and Security in Clouds", January 12, 2011.

[10]Ragib Hasan, "Security and Privacy in Cloud Computing".

[11]Pearson, S. and AzzedineBenameur, "Privacy, Security and Trust Issues Arising from Cloud Computing" IEEE Second International Conference Cloud Computing Technology and Science (CloudCom), Nov 30-Dec 3, 2010.

[12] Osama Chaudhary, Cloud Forensic and Challenges, Blog Published by digital4n6journal.com, 8 Feb 2017.

[13] Sameena Naaz, Faizan Ahmad Siddiqui, "Comparative Study of Cloud Forensics Tools", Communications on Applied Electronics (CAE) ISSN: 2394-4714, Foundation of Computer Science FCS, New York, USA Volume 5 – No.3, June 2016, page 24-30.

[14] J. Oberheide, E. Cooke and F. Jahanian, CloudAV: N-version antivirus in the network cloud, Proceedings of the Seventeenth USENIX Security Conference, pp. 91–106, 2008.

[15] R. Perry, E. Hatcher, R. Mahowald and S. Hendrick, Force.com cloud platform drives huge time to market and cost savings, IDC White Paper, International Data Corporation, Framingham, Massachusetts (thecloud.appirio.com/rs/appirio/images/IDC Force.com ROI Study.pdf), 2009.

[16] V. Roussev, L. Wang, G. Richard and L. Marziale, A cloud computing platform for large-scale forensic computing, in Advances in Digital Forensics V, G. Peterson and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 201–214, 2009.