ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A Novel Approach for Cloud as a Forensic Computing Perspective

Shachindra Kumar Dubey[*1], Prof. Ashok Verma[2]

[*1] Department Computer Science and Engineering, Gyan Ganga Institute of Technology and Sciences, Jabalpur, India

[2] H.O.D, Department Computer Science and Engineering, Gyan Ganga Institute of Technology and Sciences, Jabalpur, India

sachindrakumar000@gmail.com

Abstract

Cloud computing may well become one of the most transformative technologies in the history of computing. The benefits of 'cloud computing' increase challenges in maintaining data security and data privacy have also been recognized as significant vulnerabilities. These vulnerabilities generate a range of questions relating to the capacity of organizations relying on cloud solutions to effectively manage risk. Cloud service providers and customers have yet to establish adequate forensic capabilities that could support investigations of criminal activities in the cloud. In this paper we explore how cloud computing will impact the current tools, frameworks and procedures used or followed in forensic investigation.

Keywords: Cloud Computing, Cloud Forensics.

Introduction

Cloud computing is a rapidly evolving information technology (IT) phenomenon and its use in criminal activity is likely to grow further. Inflamed debates about the tools, terminology, definitions, standards, ethics and many other primary aspects of this emerging field have been ignited as result of this growth.

Outside of these specific definitional issues, it can be observed that a common vocabulary for describing different service models across public, private and hybrid 'cloud solutions' has started to emerge in the literature. These service models cover: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Importantly, all of these service models pose significant security and privacy risks, threats and vulnerabilities. In parallel with the emergence of the 'cloud', information security and forensic computing specialists have seen an almost exponential growth in activities related to cyber-warfare, cyber-espionage, hacktivism, cyber-crime, cyber-terrorism, information warfare and government sponsored or sanctioned use of malware and cyber attack tools.

The rise of cloud computing not only exacerbates the problem of scale for digital forensic activities, but also creates a brand new front for cyber crime investigations with the associated challenges. Digital forensic practitioners must extend their expertise and tools to cloud computing environments. Moreover, cloud-based entities – cloud service providers (CSPs) and cloud customers – must establish forensic capabilities that can help reduce cloud security risks.

This paper aims to make a contribution to these debates by exploring how differences between indiscriminate malware and targeted cyber-attack tools problematize the capacity of organizations to manage risk. This paper discusses the emerging area of cloud forensics, and highlights its challenges and opportunities.

Broad Definitions to Support Discussion

Various definitions of cloud computing have been suggested simply due to the fact that clouds have several uses presenting a mixture of services and are able to be deployed in various ways. Schubert et al., (2010) define cloud computing as:

A 'cloud' is an elastic execution environment of resources involving multiple stakeholders and providing a metered service at multiple granularities for a specified level of quality (of service).

The National Institute of Standards and Technology (NIST) Information Technology Laboratory (2011), define cloud computing as:

A model for enabling convenient, on-demand network access to a shared pool of configurable and reliable *computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal consumer management effort or service provider interaction.*

“Cyber attack *refers to deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks*”.

Cloud Forensics : A Perspective

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. Digital forensics is the application of computer science principles to recover electronic evidence for presentation in a court of law.

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.

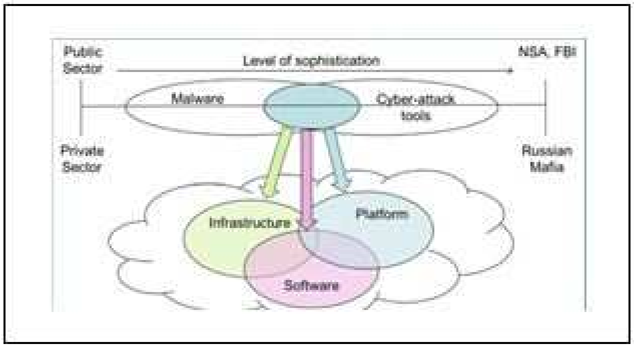

Fig:- Identifying the key source of risks for organizations adopting cloud.

In terms of real, tangible risks, it is clear that there is an area of overlap between the domains of malware and cyber-attack tools that is less easy to define in which there is a medium level of sophistication available to public and private sector players who may have a desire to target and/or attack an organization. The blue oval in given figure displays this intersection area as a starting point for examining the technical, legal and ethical issues arising from cloud computing service models.

In this ‘middle-ground’ organizations opting for cloud solutions are increasing their potential exposure to technical, legal and business risks. These risks apply in different ways across the different dimensions of cloud service models (Infrastructure; Platform; Software). From a forensic perspective, it can be argued that as increasing numbers of organizations opt for cloud solutions, there is a need to think comprehensively about what the challenges are *when* (rather than *if*) things go wrong.

A. Technical Dimensions

The technical dimension encompasses the procedures and tools that are needed to perform the forensic process in a cloud computing environment. These include data collection, live forensics, evidence segregation, virtualized environments and proactive measures.

Data collection is the process of identifying, labeling, recording and acquiring forensic data. The forensic data includes client-side artifacts that reside on client premises and provider-side artifacts that are located in the provider infrastructure. The procedures and tools used to collect forensic data differ based on the specific model of data responsibility that is in place. The collection process should preserve the integrity of data with clearly defined segregation of duties between the client and provider. It should not breach laws or regulations in the jurisdictions where data is collected, or compromise the confidentiality of other tenants that share the resources. For example, in public clouds, provider side artifacts may require the segregation of tenants, whereas there may be no such need in private clouds. Rapid elasticity is one of the essential characteristics of cloud computing.

Another essential characteristic of cloud computing is resource pooling. Multi-tenant environments reduce IT costs through resource sharing. However, the process of segregating evidence in the cloud requires compartmentalization. Thus, procedures and tools must be developed to segregate forensic data between multiple tenants in various cloud deployment models and service models.

B. Organizational Dimensions

To establish a cloud forensic capability, each cloud entity must provide internal staffing, provider-customer collaboration and external assistance that fulfill the following roles:

- Investigators: Investigators are responsible for examining allegations of misconduct and working with external law enforcement agencies as needed. They must have sufficient expertise to perform investigations of their own assets as well as interact with other parties in forensic investigations.
- IT Professionals: IT professionals include system, network and security administrators,

ethical hackers, cloud security architects, and technical and support staff. They provide expert knowledge in support of investigations, assist investigators in accessing crime scenes, and may perform data collection on behalf of investigators.

- Incident Handlers: Incident handlers respond to security incidents such as unauthorized data access, accidental data leakage and loss, breach of tenant confidentiality, inappropriate system use, malicious code infections, insider attacks and denial of service attacks. All cloud entities should have written plans that categorize security incidents for the different levels of the cloud and identify incident handlers with the appropriate expertise.
- External Assistance: It is prudent for a cloud entity to rely on internal staff as well as external parties to perform forensic tasks. It is important for a cloud entity to determine, in advance, the actions that should be performed by external parties, and ensure that the relevant policies, guidelines and agreements are transparent to customers and law enforcement agencies.

Challenges for Certain Tools and its Ethical Issues

Although cloud computing offers many benefits, there is major concern regarding cloud forensic due to lack of security, privacy and the lack of access and control over forensic data. More particularly, there are still questions to be answered relating to its ability to support forensic investigations. This section is intended to highlight the number of challenges relating to digital forensics in cloud computing.

- Forensic Data Collection:- In every combination of cloud service model and deployment model, the cloud customer faces the challenge of decreased access to forensic data. Access to forensic data varies considerably based on the cloud model that is implemented. Infrastructure as a service (IaaS) customers enjoy relatively unfettered access to the data required for forensic investigations. On the other hand, software as a service (SaaS) customers may have little or no access to such data.
- Live Forensics:-Constructing the timeline of an event requires accurate time synchronization. Time synchronization is complicated because the data of interest resides on multiple physical machines in multiple geographical regions, or the data may be in flow between the cloud infrastructure and remote endpoint clients.

  The use of disparate log formats is already a challenge in traditional network forensics. The challenge is exacerbated in the cloud due to the sheer volume of data logs and the prevalence of proprietary log formats.

  Deleted data is an important source of evidence in traditional digital forensics. In the cloud, the customer who created a data volume often maintains the right to alter and delete the data. When the customer deletes a data item, the removal of the mapping in the domain begins immediately and is typically completed in seconds. Remote access to the deleted data is not possible without the mapping.
- Vitualized Environments:-Cloud computing provides data and computational redundancy by replicating and distributing resources. Most CSPs implement redundancy using virtualization. Instances of servers run as virtual machines, monitored and provisioned by a hypervisor. A hypervisor is analogous to a kernel in a traditional operating system. Hypervisors are prime targets for attack, but there is an alarming lack of policies, procedures and techniques for forensic investigations of hypervisors.

  Investigators may unknowingly violate laws and regulations because they do not have clear information about data storage jurisdictions.

Opportunities

Despite the many challenges facing cloud forensics, there are several opportunities that can be leveraged to advance forensic investigations.

- Cost Effectiveness:-Security and forensic services can be less expensive when implemented on a large scale. Cloud computing is attractive to small and medium enterprises because it reduces IT costs. Enterprises that cannot afford dedicated internal or external forensic capabilities may be able to take advantage of low-cost cloud forensic services.
- Data Abundance:-Amazon S3 and Amazon Simple DB ensure object durability by storing objects multiple times in multiple availability zones on the initial write. Subsequently, they further replicate the objects to reduce the risk of failure due to device unavailability and bit rot. This replication also reduces the likelihood that vital evidence is completely deleted.
- Scalability and Flexibility:-Cloud computing facilitates the scalable and flexible use of resources, which also applies to forensic

services. For example, cloud computing provides (essentially) unlimited pay-per-use storage, allowing comprehensive logging without compromising performance. It also increases the efficiency of indexing, searching and querying logs. Cloud instances can be scaled as needed based on the logging load. Likewise, forensic activities can leverage the scalability and flexibility of cloud computing.

- Forensics as a Service:-The concept of security as a service is emerging in cloud computing. Research has demonstrated the advantages of cloud-based anti-virus software and cloud platforms for forensic computing. Security vendors are changing their delivery methods to include cloud services, and some companies are providing security as a cloud service. Likewise, forensics as a cloud service could leverage the massive computing power of the cloud to support cyber crime investigations at all levels.

Conclusions

This paper has commenced a discussion on the implications of cloud computing service models in relation to technical, legal and ethical issues for managing risks arising from malware and cyber-attacks. A number of data security and data privacy vulnerabilities have been identified and the implications for organizations opting for these cloud service models identified. The paper has also tried to highlight how these implications vary along a continuum of sophistication in relation to the nature, scope and scale of the attack from indiscriminate malware to the targeted cyber-attack tools.

This paper has also discussed how ‘cloud solutions’ pose additional challenges for forensic computing specialists including discoverability and chain of evidence. When things do go wrong and harm is caused, there may be limited options for technical, legal or even ethical responses open. It is anticipated that by exploring these risks and differentiating between the technical, legal and ethical issues, the paper has contributed to raising organizational awareness of the additional risks faced by organizations deciding to move to cloud solutions.

References

[1] Amazon, AWS Security Center, Seattle, Washington (aws.amazon.com/security).

[2] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, San Francisco, California (www.cloudsecurityalliance.org/csaguide.pdf), 2009.

[3] European Network and Information Security Agency, Cloud Computing: Benefits, Risks and Recommendations for Information Security, Heraklion, Crete, Greece (www.enisa.europa.eu/act/rm/files/deliverables/ cloud-computing-risk-assessment), 2009.

[4] P. Mell and T. Grance, The NIST Definition of Cloud Computing (Draft), Special Publication 800-145 (Draft), National Institute of Standards and Technology, Gaithersburg, Maryland, 2011.

[5] U.S. Department of Justice: http://www.fbi.gov/news/stories/2011/november /malware_110911.

[6] Help Net Security: http://www.net-security.org/secworld.php?id=11513.

[7] National Cyber security and Communications Integration Center: Assessment of Anonymous Threat to control Systems. US Department of Homeland, Security (2011).

[8] Ruan, K., Carthy, J., Kechadi, T., Crosbie, M.: Cloud forensics: anoverview. Adv. Digital Forensics **VII**, 35–46 (2011).

[9] Department of Defense: Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934. Department of Defense, United States of America (2011).

[10] Department of Defense: Department of Defense Strategy for Operating in Cyberspace. Department of Defense, United States of America (2011).

[11] Birk Dominik and Wegener Christoph, Technical Issues of Forensic Investigations in Cloud Computing Environments, 2011.

[12] Giova Giuliano, Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems, Internal Journal of Computer Science and Network Security, Vol. 11 No.1, January 2011.