International Journal of Innovation in Enterprise System, Volume 2, Issue 02, July 2018, pp 18-23

A Proposed Model of Digital Forensic on Cloud Computing Security Infrastructure

Mohammad Hafiz Hersyah
Computer System Department
Andalas University
Padang, Indonesia
mhafiz@fti.unand.ac.id

Corresponding author:
Received: 06 July 2017, Revised: 06 February 2018, Accepted: 15 May 2018, Published: 06 July 2018

Abstract—Over the past decades, practitioners and researchers have made remarkable achievements in digital forensic. The abilities to conquer major technical obstacles are bestowing practitioners greater access to digital evidence. Sophisticated forensic techniques and tools are being developed to assist forensic acquisition and extraction of volatile data, inspection of remote repositories system and analysis of network traffic. Computer forensic is a comprehensive work that based on several attributes that are : objectivity, relevance and legitimacy to compose a system model that projected to be an electronic evidence forensic system. Latest studies show that the rapid growing of cloud computing facilities usage that has enable various improvements as part of the innovation process at organisations. Information systems are in frequently exposed to various types of threats which able to trigger different types of bad consequences as more and more information stored, problems arise especially about security information technology risk aspects.

Keywords—computer forensic, cloud computing, electronic evidence forensic system, security, information technology risk, information system

I. Introduction

Cloud computing is a broad paradigm based on models for providing services of storage and platform software, which an emerging paradigm of computing that substitute computing as a personal usage by computing as a public domain. Cloud computing concept has emerged from distributed and grid computing domains that are already in use for mail servers, web storages and hosting services. Cloud computing, as defined by NIST, is referred to as : A model for enabling ubiquitous, convinient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storages, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[1]. Security of a cloud service should consist of authentication, authorization, confidentality, integration which basically constitute principles. Modren forensic computing, the science that delas with techniques and procedures for identifying, collecting, preserving, analyzing and presenting digital data before a court of law [2] requires a sharply increasing amount of computational resources as the number of computer related investigations continues to grow in scope of scalability, fault tolerance and collaborative processing. The significance of security field features heavilly on the life cycle of information systems. In fact, information systems nowadays are battered by individuals, organisations, goverments and system are become primary attention to inforation security attacks and would bring a catastrophic effect of lossing multiple resources that are very valuable. Moreover, criminals are becoming more aware of digital forensic and investigation cpabilities, and making more sophisticated use of computers and networks to commit their crimes. Some are even developing “anti-forensic” methods and tools specifically designed to conceal their activities and destroy digital evidence, and generally undermine digital investigations. The integration of strong encryption into operating systems is also creating challenges for forensic examiners, potentially preventing the side from recovering any digital evidence from a computer [3].

II. Cloud Computing

Cloud computing represents a convergence of two major trends in information technology – (a) IT Efficiency, whereby the power of the latest sophisticated computers is utilized more efficiently through highly scalable hardware and software resources and (b) Business agility, whereby IT can be projected as a competitive tool through rapid development, parallel batch processing, use of compute-intensive business analytic and mobile interactive applications that respond in real time to user requirements[4].

A. Advantages of Cloud Computing

Specifically, cloud computing offers the following key advantages :

- It dramatically lowers the cost of entry for smaller firms attempting to benefit from compute-intensive business analytics that were hither to available only to the largest of corporations.
- Able to provide instant access to hardware resources, without paying much attention on upfront capital investment for users, leading to a faster time to market in many business.
- Lower IT Barriers to innovation, as can be witnessed from many promising startups, from the

ubiquitous online applications such as Facebook and Youtube to more focused applications.

- Easier for enterprises to scale their services – which are increasingly reliant on accurate information. In fact, the goal of cloud computing is to scale reources up or down dynamically through software APIs depending on client load with minimal service provider interaction [5].
- Makes possible new classes of applications and deliver services that were not possible before.Example include (a) mobile interactive application (b)parallel batch processing (c) business analytic that can utilize vast amount of computer resources and (d) extensions of compute-intensive desktop applications that able to offload the data crunching to the cloud leaving only the rendering of the processed data at the frond-end, with the availability of network bandwidth reducing the latency involved [6].

Front end and Back end are two sections in a cloud system. What is seen by the user is the front end and the cloud is the back end which is connceted through the internet [7].

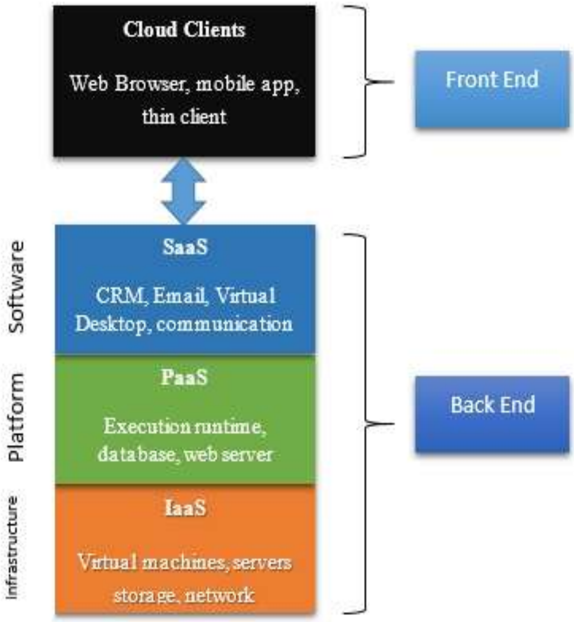
Cloud Clients
Web Browser, mobile app, thin client
Front End
Software
SaaS
CRM, Email, Virtual Desktop, communication
Platform
PaaS
Execution runtime, database, web server
Infrastructure
IaaS
Virtual machines, servers storage, network
Back End

Fig 1. Cloud Computing Architecture

There are four common deployment on cloud computing as follows :

- *Public Cloud* – The Cloud infrastructure is owned by the cloud service provider, which is exists in the premise of cloud provider. Small and Medium enterprise (SMEs) benefit to great extent from using public clouds [8].
- *Private Cloud* – Operated solely for an organization. It can be managed by the organization itself or a thrid party. The private cloud can exist on premise or off premise [9]. Advantages of private clouds are higher security and more privacy, more control, cost and energy efficiency [10].
- *Hybrid Cloud* – Is a composition of two or more clouds (private, community or public). Each of them remain as unique entities but are linked together by standarized or proprietary technology.
- *Community Cloud* – Shared by several organizations which have shared concerns (e.g., mission, security requirements, policy and compliance consideration).

III. Cloud Computing Security Architecture

With all the advantages of cloud paradigm and its potential for decreasing cots and reducing the time required to start new initiatives, cloud security will always be a major concern. The objectives of cloud security controls is to reduce vulnerabilities to a tolerable level and minimize the effects of an attack. A variety of factors affect the implementation and performance of cloud security architecture. There are general issues involving regulatory requirements, adherence to standars, security management, information classification and security awareness. Then, there are more spesific architecturally related areas including trusted hardware and software, providing for a secure execution environment, establishing secure communication and hardware augmentation through microarchitecture.

An organizations must determine what impact an attack might have, and the likelihood of loss. Examples of loss are compromise of sensitive information, financial embezzlement, loss of reputation and physical destruction of resources. There are generly four kind of control [11].

- ***Deterrent control –*** Reduce the likelihood of deliberate attack.
- ***Prevantive controls –*** Protect vulnerabilities and make an attack unsuccessful or reduce its impact. Preventive controls inhibit attempts to violate security policy
- ***Corrective controls –*** Reduce the effect of an attack
- ***Detective controls –*** discover attacks and trigger preventive or corrective controls. Detective controls warn of violations or attempted violations of security policy and include such controls as intrusion detection system, organizational policies, and motion detectors.

In cloud environment, applications are run on different servers in a distributed mode. These applications interact with outside world and other applications and may contain sensitive information whose inappropriate access would be harmful to a client. In addition, cloud computing is increasingly being used to managed and store huge amounts of data in database applications that are alse co-located with other users information.

A. Infrastructure Security : The Network Level

When looking at the network level of infrastructure security, it is important to distinguish between public clouds and private clouds. With private clouds, there are no new attacks, vulnerabilities or change in risk spesific to this topology that information security personel need to consider. Although the organization's IT architecture may change with the implementation of a private cloud, current network topology will probably not alter significantly [12].

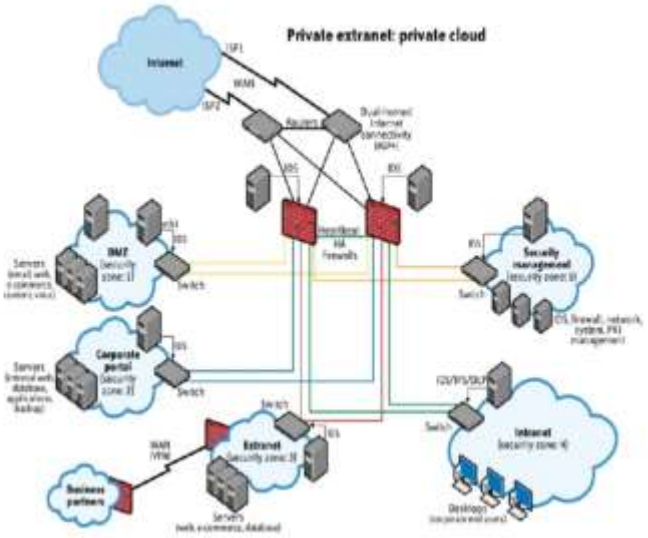
Private extranet: private cloud
Internet
ISP1
WAN
ISP2
Routers
Dual-homed Internet connectivity (BGP)
IDS
IDS
HA Firewalls
DMZ (security zone 1)
Switch
Corporate portal (security zone 2)
Switch
Security management (security zone 5)
Switch
Extranet (security zone 3)
Switch
Intranet (security zone 4)
Switch
IDS/IPS/DLP
WAN (VPN)
Business partners
Servers (web, e-commerce, database)
Desktops (corporate end users)

Fig 2. Generic Network Topology for Private Cloud.

There lists security control at network level

TABLE 1. SECURITY CONTROL AT NETWORK LEVEL

Threats outlook	Low (With the exception of DoS attacks)
Preventive controls	Network access control supplied by provider (e.g., firewall,)encryption of data in transit (e.g., SSL, IPSec)
Detective controls	Provider-managed aggregation of security event logs (security incident and event management, or SIEM), network-based intrusion detection system / intrusion prevention system (IDS/IPS)

B. Infrastructure Security : The Host Level

Consideration regarding the context of cloud service delivery models (SaaS, PaaS, IaaS) and deployment models (public, private and hybrid) should take into account. Although there are no known new therats to host that are spesific to cloud computing, some virtualization security threat such as VM escape, system configuration drift and insider threat by way of weak access control to the hypervisor carry into the public cloud computing environment.

The simplicity of self-provisioning new virtual server on an IaaS platfrom create a risk that insecure virtual server will be created. Securing the virtual server in the cloud requires strong operational security procedure coupled with automation of procedures as follows.

- Use a secure-by-default configuration. A best practice for cloud-based applications is to build custom VM Images that have only the capabilities and service necessary to support the application stack.
- Track the inventory of VM images and OS versions that are prepared for cloud hosting
- Protect the integrity of the hardened image from unauthorized access.
- Safeguard the private keys required to access hosts in public cloud.
- Isolate the decryption keys from the cloud where the data is hosted.
- Include no authentication credential in virtualized images except for a key to decrypt the filesystem key.
- Do not allow password-based authentication for shell access.
- Run a host firewall and open only the minimum ports necessary to support the services on an instance.

C. Infrastructure Security : The Application Level

Application or software security should be a critical element of a security program. Most enterprise with information security program have yet to institute an application security program to address this realm. It has been a common practice to use a combination of perimeter security control and network and host based access control to protect web application deployed in a tightly controlled environment. Including corporate intranets and private clouds.

Web application deployed in apublic cloud must be designed for an internet threat model and security must be embedded into the software development life cycle (SDLC).

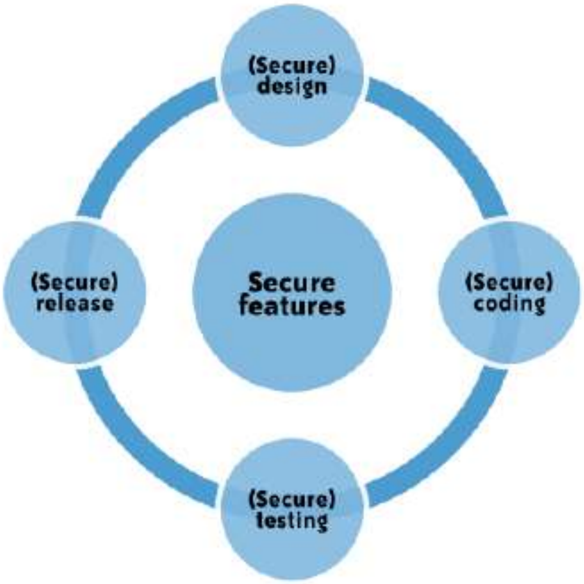

Fig 3. Software Development Life Cycle for web application in cloud

IV. RISK IT - *ISACA*

The risk management process model groups key activities into a number of process. These proceeses are grouped into three(3) domains. The domains are [13]:

- Risk Governance – ensure that IT risk management practices are embedded in the enterprise, enabling it to secure optimal risk-adjusted return. There are several activities within this section that are :
  - Establish and maintain a common risk view.
  - Integrate with ERM.
  - Make risk-aware business decision.
- Risk Response – ensure that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities. Several break down activities within this secation are :
  - Articulate Risk.
  - Manage Risk.
  - React to events.
- Risk Evaluation – ensure that IT-related risks and opportunities are identified, analysed and presented in business term. The break down activities within this section are :
  - Collect data.
  - Analyze Risk.
  - Maintain Risk Profile.

V. DIGITAL FORENSIC

There are four phase of digital forensic as follows [14] :

- *Collection* – Data are identified, labeled, recorded and aquired from all of the possible sources of relevan data, using procedures that preserve the integrity of the data
- *Examination* – The data are collected should be examined using a combination of automated and manual methods to assess and extract data of particular interest for the spesific situation, while preserving the integrity of the data
- *Analysis* – The Result of the examinations should be analyzed, using well-documented methods and techniques, to derive useful information that addresses the questions that were the impetus for the collection and examination
- *Reporting* – The results of the analysis should be reported. Items to be reported may include the following : (a) a description of the actions employed (b) an explanation of how tools and procedures were selected (c) a determination of any other actions that should be performed, such as forensic examination of additional data sources, securing identified, vulnerabilities and improving existing security control and recommendations for improvemnets to policies, guidelines, procedures, tools ad other aspects of forensic process.

Collection
Examination
Analysis
Reporting

Fig 4. Phases of Digital Forensic

A. *Forensic Artifacts in Cloud Environment*

Similar to traditional computer system stack, a list of forensic artifacts and its order of volatility need to be identified and spesified for the cloud system stack [15].

- *Physical Layer* – Includes hardware computing resources such as computers (CPU and memory), networks (routers, firewalls, switches, network links and interfaces) and storage components (hard disks) and other physical computing infrastructure elements, as well as facility resources such as heating, ventilation and air conditioning (HV AC), power, communications and other aspects of the physical plant.
- *Abstarction Layer* – The resource abstraction and control layer contains the system components that cloud providers use to provide and manage access

to the physical computing resources through software abstraction. Resource abstraction components typically include software elements such as hypervisors, virtual machines, virtual data storage and other computing resource abstraction.

- *Service Layer* – The service layer is where cloud providers define *interfaces* for cloud consumers to access the computing services. Access interface of each of three service models are provided in this layer. It s possible, though not necessary, that SAAS applications can be built on top of PaaS components and PaaS components can be built on top of IaaS components.
- *OS Layer (IaaS)*- The IaaS interface can also be called OS (Operating System), as this layer of iterface provides interfaces to access operating system and drivers.
- *Middleware Layer (PaaS)* – This layer provides software building blocks (e.g., Libraries, Database and Java Virtual Machines) for developing application software in the cloud.
- *Application Layer (SaaS)* – This layer of interface includes software applications targetted at end users or programs.

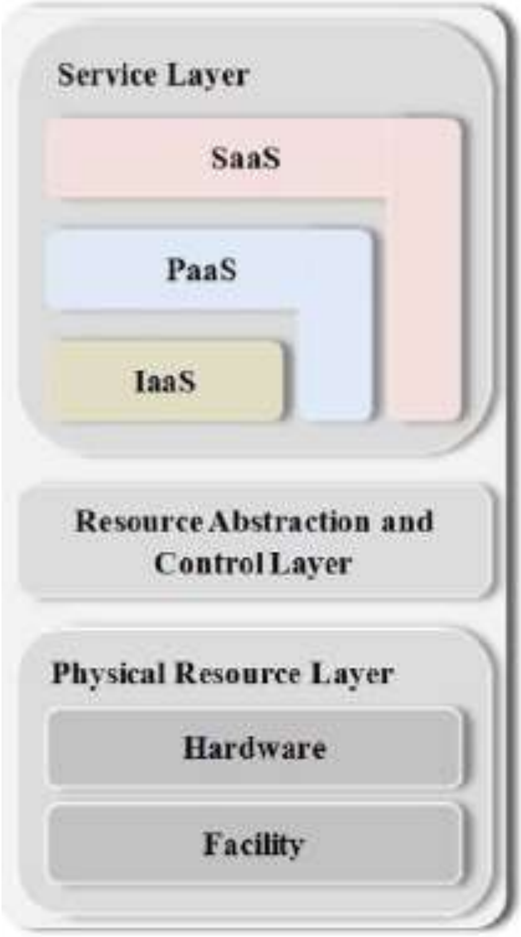

Fig 5. Cloud System Environment

B. Forensic Analysis

Forensic analysis of digital evidence depends on the case context and largely relies on the knowledge, experiece, expertise, thoroughness and in some cases the curiousity of the practitioner perfeorming the work. Although every forensic analysis will have differing aspects based on the dataset, objectives, resources and other factors, the underlying process remains fundamentally the same [16].

- ***Gather information and make observation –*** Sometimes refferd to as forensic examination and involves verifying the integrity and authenticity of the evidence, performing a survey of all evidence to determine how to proceed most effectively and doing some preprocessing to salvage deleted data, handle special files, filter out irrelevant data and extract embedded metadata.
- ***Form a hypothesis to explain observation –*** While forensic practitioners are gathering information about crime under investigation, we develop possible explanantions for what we are observing in the digital evidence

- ***Evaluate the hypothesis* –** Various predictions will flow naturally from any hypothesis (if the hypothesis is true, then the possibilities to find x in the evidence is bigger). Beside that, to determine whether such expectations are borne out by the evidence.
- ***Draw conclusions and communicate findings* –** Once a likely explanation of events relating to a crime has been established, forensic pratitioners must convey the work to decision making phase.

VI. Discussion

Based on types of cloud deployment models, forensic implication in technical, organizational dan legal dimension are analyzed.

TABLE 2. CLOUD ARCHITECTURE AND ITS FORENSIC IMPLICATION

Types	**Digital Forensic Implication**
Public	1. Allow anonymous usage 2. Personal Indentiable Information issues 3. Provider capabilities in evidence acquisition 4. Limited multiple jurisdictions
Private	1. Downgrade security forensic 2. Complete Risk Management Assessment
Hybrid	1. Evidence segregations
Community	1. Complex security implication 2. Complex forensic implications

From the implications above, there is a proposed model of digital forensic on cloud computing architecture that sould be suit on every deployment type of cloud on fig 6.

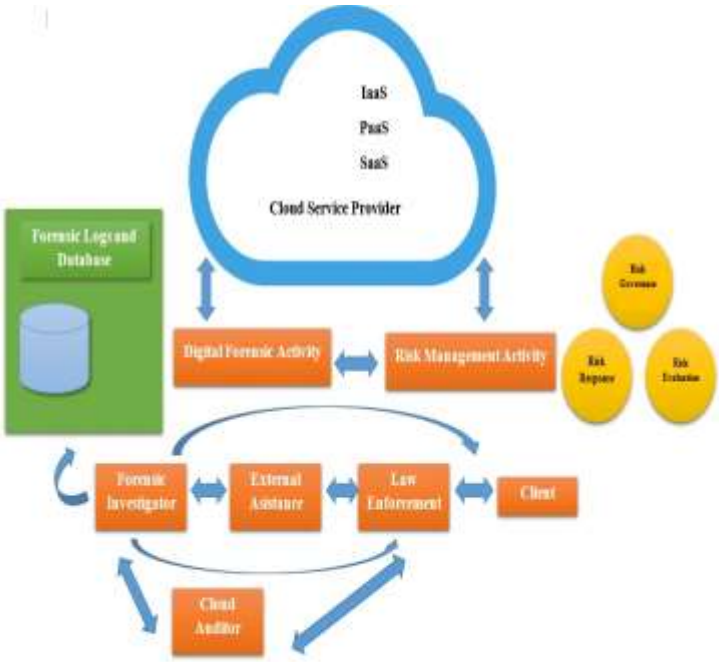

Fig 8. A Proposed model on Digital Forensic in Cloud Computer Architecture

VII. Conclusion and Future Works

The proposed model is flexible to be applied at four different type of cloud computing that are (a) Public (b) Private (c) Hybrid (d) Community.

Future works from this publication is start to write paper regarding virtualization on cloud computing and its digital forensic.

Acknowledgment

I would like ekspress acknowledgment to my department, Computer System – Information Technology Faculty, Andalas University, My Colleagues and My Family.

References

[1] P.Mell. T. Grance, the NIST definition of cloud computing in National Institute of Standars and Technology, Gaithersburg. MD 20899-8930, springer, 2011, pp 1-7

[2] McKemmish R. What is forensic Computing. *Trends and Isuues in Crime and Criminal Justice;n 118;1999*.

[3] Casey, E & Stellatos G The Impact of full disk encryption on digital forensic ACM SIGOPS Operating System Review 2008 42(3)

[4] Kim W. Cloud Computing : Today and Tomorrow, Journal of Object Technology 8(1) (2009) 65-72

[5] DubeyA, Wagle D Delivering software as a service, The McKinsey Quarterly (May 2007) 1-12.

[6] Marston S. Li Z, Bandyppadhyay S, Zhang J, Ghalsasi A. Cloud Computing – The Business perpective, Elseviewer, 2010.

[7] Strickland, Jonathan. "How Cloud Computing Works" http://computer.howstuffworks.com/cloud-computing/cloud-computing.htm.

[8] Rajkumar Buyya, Christian Vechioa. Tharamai Selvi, Mastering Cloud Computing, McGraw Hill pp 112-117.

[9] Kevin Kelly : A Cloudbook Bible, Wiley Publishing Inc pp 6-9

[10] http://www.tutorialspoint.com/cloud-computing/.

[11] NIST Spesial Publication 800-30,"Risk Management Guide for Information Technology Systems," July 2002.

[12] Mather Tim, Kumaraswamy, Subra, Latif Shahed 'Cloud security and privacy : an Enterprise Perspective on Risks and Compliance O'Reilly 2009

[13] The Risk IT Framework, ISACA, 2009

[14] Sammons, John Digital Forensics ; Threatscape and Best Practices. Syngress – Elsevier 2015.

[15] Liu, F., Tong, J.,Mao, J.,Bohn, R.,Messina, J.,Badger, L.,Leaf, D NIST Cloud Computing Reference Architecture – National Institute of Satndards and Technology. Spesial Publication 500-292(2011).