Cloud Forensics Challenges from a Service Model Standpoint: IaaS, PaaS and SaaS

David Freet
Eastern Kentucky University,
521 Lancaster Ave,
Richmond, KY, USA
david.freet@eku.edu

Rajeev Agrawal
North Carolina A&T State University,
1601 E Market St,
Greensboro, NC, USA
ragrawal@ncat.edu

Sherin John
North Carolina A&T State University,
1601 E Market St,
Greensboro, NC, USA
sjohn@aggies.ncat.edu

Jessie J Walker
University of Arkansas at Pine Bluff
1200 N. University Dr.
Pine Bluff, AR, USA
walkerjj@uapb.edu

ABSTRACT
Cloud computing is a promising and expanding technology which could replace traditional IT systems. Cloud computing resembles a giant pool of resources which contains hardware, software and related applications, which can be accessed through web-based services on a pay-per-usage model. The main features of the cloud model are accessibility, availability and scalability, and it can be subdivided into three service models: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Cloud computing continues to transform how security challenges are addressed in closed and private networks. Given the advanced functionality offered by cloud computing, network monitoring and digital forensics efforts are potentially detectable and service-interruptive, which significantly impacts the effectiveness and thoroughness of digital forensic methods. This paper presents a general view of cloud computing, which aims to highlight the security issues and vulnerabilities associated with cloud service models. The technology is mainly based on virtualization, where data is always volatile and typically stored in a de-centralized architecture located across various countries and regions. This presents forensics investigators with legal challenges, due to the nature of multi-tenancy and distributed shared resources. This paper examines the three cloud service models and discusses the security challenges and issues involved with each service model along with potential solutions for each.

General Terms
Management, Performance, Design, Reliability, Experimentation, Security, Human Factors, Theory, Legal Aspects.

Keywords
Cloud computing, IaaS, PaaS, SaaS, Cloud forensics.

1. INTRODUCTION
In recent years, cloud computing has revolutionized how information is processed by providing a scalable, cost-effective and efficient technology platform. From a technology management standpoint, cloud computing offers additional computing power and more storage at a lower cost. A study by Market Research Media states that the global cloud computing market is expected to grow at a 30% Compound Annual Growth Rate (CAGR) reaching $270 billion in 2020 [1]. However, the characteristics that make cloud computing so powerful also make cloud-based crimes and attacks on clouds and their users more difficult to prevent and investigate [2]. While cloud technology provides a distinct competitive advantage to many organizations, a recent report found that 52 percent of large companies and one-third of small and medium businesses are not moving to the cloud because of security concerns [3].

Cloud computing is an on-demand, pay-per-use computing architecture that delivers computing resources as services over the Internet. This technology provides a preconfigured infrastructure at a lower cost and allows users to utilize software or hardware resources which are owned and managed by a Cloud Service Provider (CSP) at remote locations. The three service models available in cloud technology are Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). By using cloud services, companies can eliminate the hazards and costs involved with the installation and management of traditional IT infrastructure. The user is charged for the services consumed as with utility-based computing.

According to Gartner, Inc., the year 2016 will be a defining year for cloud computing as private clouds begin to give way to hybrid clouds, and nearly half of large enterprises will have hybrid cloud deployments by the end of 2017 [4]. While cloud services are gaining high popularity in the e-business world, IT departments are allocating billions of dollars to take advantage of cloud-based services. With all the benefits of cloud technology, it still faces major problems with security issues and challenges in forensic investigations. There has traditionally been a wide gap in budget spending for the newest cloud technology, and investment in research and methods to keep the security of the cloud in step with the rate at which the technology itself is growing.

2. BACKGROUND
The five characteristics of the cloud computing model are on-demand self-service, global network access, location-independent resource pooling, rapid elasticity, and pay per use. Cloud environments can be classified into four deployment models: private, public, hybrid and community cloud. A single cloud datacenter consists of computing nodes, switches, network topology, storage nodes, front-end jobs, physical resource sets and software services [5]. Server virtualization comprises the backbone of cloud architecture. Through server virtualization, a service provider can allocate physical resources among multiple

MEDES '15, October 25-29, 2015, Caraguatatuba, Brazil
 ISBN 978-1-4503-3480-8/15/10…$15.00
http://dx.doi.org/10.1145/2857218.2857253

customers. Amazon Elastic Compute Cloud (EC2) and Google App Engine are the leading cloud service providers in the market.

2.1 Five Essential Characteristics of Cloud Computing

2.1.1 On-demand self-service

On-demand self-service refers to the service provided by cloud computing vendors that enables the provision of cloud resources on demand whenever they are required. The user can scale the required infrastructure up to a substantial level without disrupting the host operations. Resources such as server time, applications, e-mail and network storage can be automatically allocated and used as needed without interaction from the CSP. Cloud service providers that deliver on-demand self-services include Microsoft, Amazon Web Services (AWS), IBM, Google and Salesforce.com.

2.1.2 Broad network access

In cloud technology, network access and capabilities are available through a web browser, and can be accessed through standard devices such as cell phones, tablets, laptops and workstations.

2.1.3 Resource pooling

Cloud computing resources such as virtual machines, bandwidth, memory, storage devices, and processing power are dynamically allocated and assigned to multiple customers using a multi-tenant model. As it is a location-independent technology, the customer does not have any control or information about the exact location of the given resources. However, the information about the location is available at a higher level of abstraction.

2.1.4 Rapid elasticity

Depending on customer demand, cloud services can be quickly and elastically provisioned and scaled up or down at any time.

2.1.5 Measured service

Cloud computing services and resources can be automatically measured, controlled, and monitored. Therefore, it ensures transparency to both the provider and consumer as to the nature and degree of utilized services. Cloud technology uses a metering capability which is helpful to customers to control and optimize resource usage. It is similar to a pay-per-use model as seen with electricity or municipality water bills.

These are the five essential characteristics [6] which should be provided by a cloud computing vendor. Some vendors may fail to provide one or more of the essential characteristics. Therefore, customers need to determine a proper Service Level Agreement (SLA) that dictates a guaranteed level of usability for cloud services.

3. CLOUD FORENSICS

The relationships between computer forensics, network forensics and cloud forensics are sometimes loosely defined. Cloud forensics intersects network forensics and computer forensics under the umbrella of digital forensics and involves the investigation of the whole cloud computing environment including cloud service providers (CSP), data infrastructure, network, memory storage, and virtualized services [7]. With traditional digital forensics on computer systems, analysis, threat monitoring and evidence collection is performed inside the system where the process is loaded in memory, on the hard disk like other applications, and must be queued to perform its duties. Current malware engines are able to detect such processes and react by hiding, replicating to other areas on the disk, and modifying the evidence collected. Operating from within the system exposes the administrator's efforts of detecting and responding to attacks. Common digital forensic techniques involve investigating systems in either a live or dead state, with the former being a common practice. In a dead state, the system is shut down abruptly or procedurally. Both methods create either an out-of-sync state for evidence or potential for modification of the evidence. In an abrupt powering off of the system to capture a snapshot of the system, data left in cached storage is unable to be synchronized with data stored on the disk storage devices or in the application's data stores. Investigating a system in a live state addresses the loss of data in memory and cached storage. However, the monitoring requires that the tool must be loaded on the hard drive and, when active, in memory.

4. CLOUD FORENSICS CHALLENGES

Traditional means of threat monitoring and evidence collection for digital systems may not work effectively on cloud-based systems running on virtual machines. Analysis, monitoring and evidence collection of processes loaded in memory and on hard disks must be performed differently on a cloud-based system. Malware engines are able to detect traditional processes and react by hiding, replicating to other areas on the disk, and modifying collected evidence [7]. When operating from within the system, the administrator's efforts to detect and respond to attacks may be exposed. A technology is needed that is undetected by attackers, is non-interruptive to the main process of the system, ensures integrity of the evidence collected and its chain of custody, and remains isolated but is secure and functional as a virtual machine monitor [7]. Figure 1 lists some of the differences between traditional and cloud forensics

.

Traditional Forensics	**Cloud Forensics**
Physical access to resources	De-centralized resources with no access
Ownership of resources and logs	CSP owns resources and logs
Resources and data segregated among users	Multi-tenancy
Established forensic tools	Limitation of available tools
Non-cloud environment	Dependence on cloud services (IaaS, SaaS, PaaS)
Data access and established policies	Multi-user access policies, various geographical legal standards

Figure 1. Comparison of traditional vs. cloud forensics

The current digital forensic landscape has changed because of the introduction of new cloud-based computing platforms, particularly with respect to incident handling and forensic methods. The ability to physically acquire objects in these new virtual environments, where disks, memory and networks are shared, and traditional ownership boundaries are not clear offers numerous research opportunities, particularly within the vast domain of digital forensics. Research within the domain of cloud forensics is deficient particularly in tools, processes, and methodologies to obtain legally defensible digital evidence in the

cloud. Acquiring digital artifacts in the cloud presents unique challenges predominantly in artifact preservation, presentation in a court of law or internal investigation of user misuse.

Security and privacy are the major challenges in cloud computing. In traditional IT systems, forensic investigators have full access to the whole infrastructure. However, in cloud computing they may not be able to locate the corrupted data due to its distributed nature. The major cloud forensics challenges are Anything-as-a-Service (XaaS), forensic data acquisition challenges, identification, collection, logging issues, legal challenges, and technical challenges. The six different infrastructure layers found in the three service models are network, servers, operating system, data, application, and access control layers [2]. The access control to each service layer is shown in figure 2.

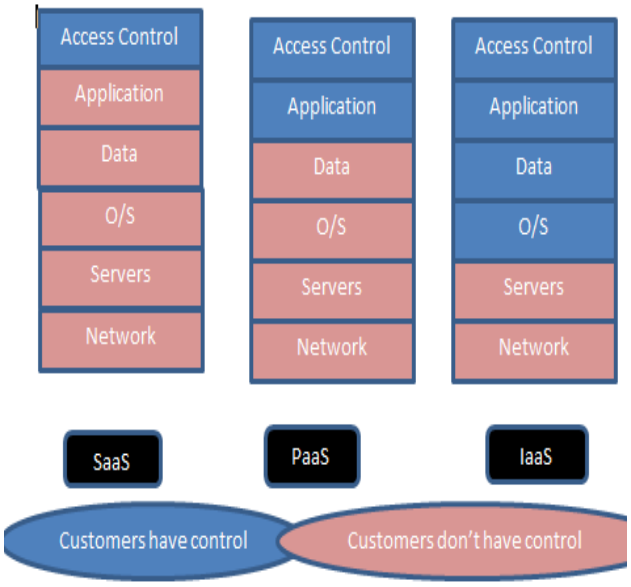

Figure 2. Customers' control over different layers in different service models

Gartner [8] has warned that "Investigating inappropriate or illegal activity may be impossible in cloud computing. Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers. If you cannot get a contractual commitment to support specific forms of investigation – along with evidence that the vendor has already successfully supported such activities – then your only safe assumption is that investigation and discovery requests will be impossible." Cloud forensic procedures will vary in accordance with the three service models. SaaS and PaaS have very limited control over process or network monitoring, whereas more control can be gained in IaaS by employing forensic-friendly logging mechanisms and VM images and snapshots from the CSP [9]. Application logs can only be obtained from customers in PaaS, whereas in SaaS customers do not receive network, database or operating system logs unless it is provided by the CSP [9].

The responses of a detailed survey on current cloud forensics challenges are shown in Figure 3 [10]. The survey includes responses from academics, practitioners, cloud service providers and industry. According to the survey, the top five challenges for cloud forensics are, jurisdiction, investigating external chain of dependencies of the CSP, lack of international collaboration and legislative mechanism in cross-nation data access and exchange, lack of law/regulation and slow advisory, and decreased access to and control over forensic data at all levels from the customer side.

4.1 SaaS Service Model

4.1.1 SaaS Challenges

SaaS can be defined as a service delivery model that delivers IT applications to end users over the Internet. According to Paul et al [11], the SaaS model is analogous to a client-server model, except that the server is replaced by the provider's data center and the resources can be accessed through web browsers (HTTP/HTTPS). The user accesses the application through a browser interface but does not have access to the underlying architecture such as network, servers, operating systems, and storage. In traditional software distributions, users must purchase and install the software on their personal computer. In the SaaS model, the CSP controls different application layers including hardware, operating system, middleware and application. The user only has access to selected applications which are "rented" from the CSP. The cloud provider makes an instance of the application, and the customer connects and uses the application through an API. Only CSPs can configure, update and manage the operations of the application and access the log files. Customers cannot access the middleware, operating system layer, or hardware layer, and have no access to the hardware log files. SaaS allows organizations to access business services via the Internet with pay-as-you-go pricing and eliminates the need for organizations to handle the installation, maintenance and software updates. The key characteristics of SaaS models are multi-tenant architecture, easy customization and improved access. The advantages of using the SaaS model include easier administration, patch management, easier collaboration, compatibility, and global accessibility.

According to Birk and Wegener [12], digital evidence can be collected at three distinct states: at rest, in motion, and in execution. Data which is stored on a hard disk or other static media can be defined as data at rest. Data that is able to transfer from one state to another can be defined as data in motion. Some data is executable, and can be used for analyzing data at rest and data in motion. There is a limited number of user-specific application configurations allowed in the SaaS model. Moreover, any installation or configuration of a forensic toolkit is impossible in an SaaS environment which makes digital evidence collection extremely difficult. In most situations, the investigator has to depend on the CSP to obtain log files, which have high importance in forensic investigations. Application logs, process logs and network logs have a major role in analyzing malicious user activities. In a distributed environment, the log files are not located in any particular system. Due to the volatile nature of VM technology, some log files cannot be recovered after the VM is powered off. SaaS service models are built upon PaaS and IaaS models. Therefore, the challenges involved with the previous models are inheritable to SaaS. This factor all lead to the consideration that the SaaS customer has no access to system logs and, consequently, has no opportunity to analyze log information in a malicious incident or offer any kind of repudiation for incidents occurring during system usage.

4.1.2 SaaS Solutions

In the SaaS model, the applications and sensitive data are stored in a vendor's datacenter. Therefore, the data stored in this cloud model is more vulnerable to the activities of malicious users. The

use of strong encryption techniques such as Secure Socket Layer (SSL) and Transport Layer Security (TLS) can reduce the vulnerability of data. A secure web application scanner that analyzes code vulnerabilities should be placed in SaaS environments and kept current with a database of the most recent vulnerabilities. Examining HTTP requests and responses with a strong firewall can help mitigate malicious network traffic but will not be able to identify code-level vulnerabilities presented within the web application.

Researchers at the Hewlett Packard Laboratory in Bristol, U.K. are developing "cells" that could be used to automate security management in the cloud. These cells could be sold as Cell-as-a-Service (CaaS). A cell would represent a single administrative domain using the same common security policies and would help mitigate the risk of an intrusion, viruses, attacks or malicious behavior [14]. Lie Detector is a similar approach to identifying potential security risks in the VM space. With the assistance of introspection software on the border of VM space, Lie Detector

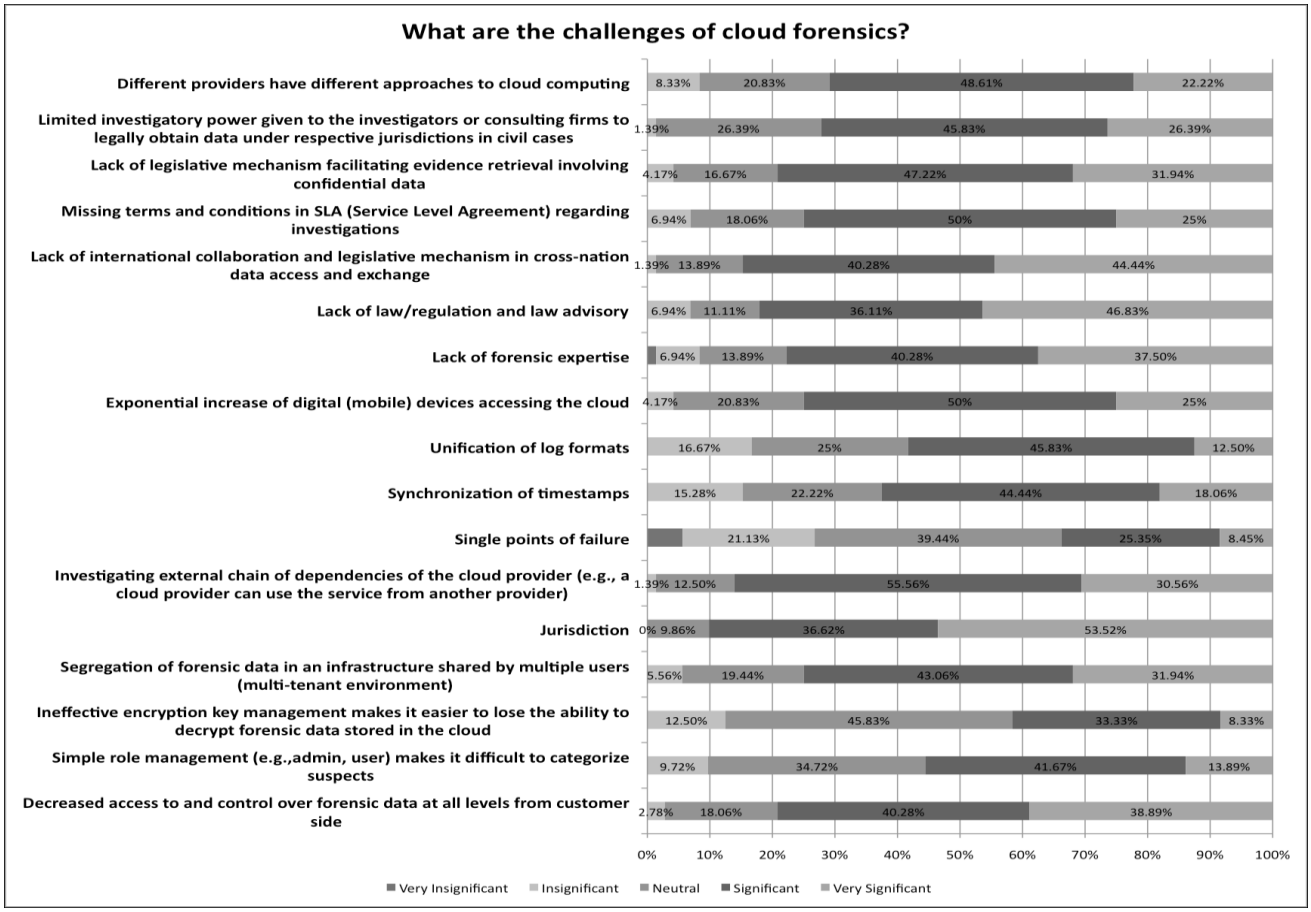

Figure 3. Challenges in cloud forensics.

With SaaS, forensic investigations are dependent solely on the CSP for obtaining the application log. This can provide legal challenges as clients may question the integrity of these logs by claiming that forensic investigators or the prosecution and the CSP have colluded to plant evidence or misrepresent log information [9]. Within the SaaS model, users send commands to the cloud server and once processed the server makes its own logs of all activities. In a forensic investigation scenario it is possible to obtain logs from the CSP, but this can depend on the CSP's willingness to cooperate and also the ease with which the log data can be located and processed. The SaaS architecture should include a mechanism whereby users keep a synchronous set of logs that can be reviewed either independently or in conjunction with those of the CSP. In order to verify authenticity, local log files can be run through a hash algorithm so that any modification of log contents can be detected [13].

can detect all running processes in the VM and can identify any views of open sockets, display the number of files on disk, and list loaded kernels [14]. By utilizing probes and comparing sets of lists, Lie Detector can improve the probability of detecting malware in the VM environment.

At the customer datacenter level, ensuring trusted security configurations with each of the clients is a best practice for ensuring VM security. CSPs must keep consistent, up-to-date security controls and provide SLAs to customers in order to ensure availability, performance and scalability. The use of strong network traffic encryption techniques such as Secure Socket Layer and the Transport Layer Security can mitigate security issues at the network layer [15]. CSPs should adhere to cloud security standards that are provided by approved agencies.

4.2 IaaS Service Model

4.2.1 IaaS Challenges

The IaaS model helps clients to modernize and expand their IT capabilities without spending capital resources on infrastructure. IaaS can be considered as the first layer and foundation of the cloud computing service model, providing a computing infrastructure platform which includes virtual server space, bandwidth, network connections, IP addresses and load balancers.

The client can access these components to build their own IT platforms. The CSP ensures infrastructure services and all other maintenance related to these services. In IaaS, the CSP allocates resources as virtual machines (VMs) and it is controlled by the hypervisor or virtual machine monitor (VMM). The CSP monitors the hypervisors and customers rent access to the guest OS running on a given VM. IaaS provides the most management options compared with other models by replacing a company's on-site IT infrastructure, especially storage, servers and networks, and putting these services in a remotely accessible cloud. With IaaS, the customer does not need to control or manage the underlying layers but has control over operating systems, storage and deployed applications. The main advantages of IaaS are scalability, pay-as-you-go pricing, location independence, physical security of data center locations, and no single point of failure.

The six layers of an IaaS cloud environment include guest application/data layer, guest OS, virtualization, host OS, physical hardware and network layer. In IaaS, customer administrative control is only in layer 5 (guest OS) and layer 6 (guest application). Table 1 explains the different data acquisition methods and trust levels for each layer [16]. While performing a forensic examination, the investigator should check the evidence in each layer separately to avoid causing inconsistency and anomalies in correlating evidence.

With the layered approach, investigators can select a layer in accordance with a desired forensic process in order to encourage integrity in examination methods. For example, packet captures can occur at the network layer, physical files at the physical layer, and hardware or virtual files at the Host OS layer [16]. Forensic tools such as EnCase Enterprise, Prodiscover, AccessData FTK, Safe Back, SnapBack, and DatArrest are powerful and easy to use remote investigation solutions used in cloud computing.

Cloud computing depends on the IaaS layer for data storage, processing power, and other shared resources. Compared with SaaS and PaaS models, IaaS has more control over the infrastructure layers such as the operating system, data, application and access control [17]. Volatile data will be lost when the VM turns off if the image of the instance has not been saved. Persistent storage environments like Amazon S3 and Amazon EBS should be used for data storage as these services provide forensic images called snapshots. Snapshots are very helpful while doing forensic investigations as there is no need to stop the system while running crucial business processes.

Sharing network infrastructure among different customers within the same server increases the possibility of vulnerabilities. VM boundaries are not secured if the VM is not isolated from other VM resources [18, 19]. The hypervisor isolates the VM from physical machines and is the key to accessing VM resources. Any compromise of the hypervisor can lead to many security issues. In a shared resource, the VM data packets are coming and going through the host machine so any compromise on the host impacts the security of the entire architecture. Even though each VM is isolated from other VMs on the same physical machine, any compromised VM can attack another VM in the network due to its shared nature. Additionally, any hypervisor misconfiguration makes Denial of Service possible as it allows one VM to use all system resources at the expense of other VMs on the network [20, 21].

The cloud infrastructure has different data centers located among different geographical regions. These centers are connected through local area networks and other high speed network connections. Therefore, any vulnerability associated with the Internet such as DDOS, MITM, IP spoofing, or port scanning is inheritable in cloud environments. Another challenge is network monitoring, which is comparatively difficult in cloud infrastructures when compares to traditional network systems.

4.2.2 IaaS Solutions

The IaaS service model gives more information about malicious activities than SaaS or PaaS models because the customer can install or set up virtual images to collect forensic evidence. Hence log files, which have prime importance in forensic investigations, can be obtained with this model. Birk and Wegener [22] proposed a system where CSPs could provide network, process, and access logs to customers through a read-only API. Dykstra and Sherman [23] recommended a cloud management solution to be used in IaaS models where customers and investigators can collect VM images, network, process and database logs, and other digital evidence which cannot be collected in other ways.

Zawoad, Dutta, & Hasan [9] introduced Secure-Logging-as-a-Service (SecLaaS), which stores virtual machine logs and provides access to forensic investigators while ensuring the confidentiality of cloud users. This technology also prevents tampering and protects log integrity by preserving proof of past logs. Legal challenges may arise as clients can question the integrity of these logs by claiming that forensic investigators or the prosecution and the CSP have colluded to plant evidence or misrepresent log information. Termination of a VM will not prevent retrieval of critical logs, as SecLaaS stores log entries in a log database and proof of entry in a proof database. This ensures that cloud users' logs are preserved in persistent storage, which prevents malicious parties from producing false copies of past logs [9].

Table 1. Six layers of the IaaS cloud environment and potential forensic acquisition techniques for each, including the cumulative trust required by each layer			
Layer	Cloud Layer	Acquisition method	Trust required
6	Guest application/data	Depends on data	Guest operating system (OS), hypervisor, host OS, hardware, network
5	Guest OS	Remote Forensic Software	Guest OS, hypervisor, host OS, hardware, network
4	Virtualization	Introspection	Hypervisor, host OS, hardware, network
3	Host OS	Access Virtual Disk	Host OS, Hardware, network
2	Physical hardware	Access physical disk	Hardware, network
1	Network	Packet capture	Network

Other solutions have included a log management system that establishes an encrypted transport layer to transfer log information to a central log collector [24], and logging capabilities provided by OS and the security logs [25].

Private Virtual Infrastructure (PVI) separates security responsibilities between the service provider and the customer. The service provider assumes responsibility for physical and logical security within the infrastructure and the consumer is responsible for ensuring the security of their virtual datacenter, including firewalls, intrusion detection systems, and monitoring and logging [14]. Both parties exchange information with each other and sometimes with a third party, as this can provide for a robust security awareness scenario based on SLAs while utilizing IPsec or SSL tunneling to secure communications between the CSP and the customer [26].

In order to overcome utility computing challenges, some technologies such as Amazon DevPay or WS-Security can be implemented with cloud web services. To prevent hacking among VMs, tools like Terra or TVDc can be used. Installing Virtual Private Networking can be useful for keeping confidentiality and integrity in place on the network. Security Virtual Machine (SVM) provides analysis for all virtual networks. Anti-DDoS virtualized OSs are helpful to prevent DDos attacks. Trusted Cloud Computing Platform (TCCP) ensures confidentiality and integrity of IaaS services, and it prevents an authorized administrator from performing malicious activities in VM environments. TCCP ensures the service backend is running on a trusted platform before launching a VM. Another feature, Trusted Platform Module (TPM), strengthens grid security, and it provides cryptographic credential, integrity protection and remote attestation.

4.3 PaaS Service Model

4.3.1 PaaS Challenges

Software companies are the primary users of PaaS to host and develop their software applications. Software producers need platforms such as physical servers, databases and web servers to run their products. In a traditional model, the company has to spend much time and labor to build their own platform to run the software applications and also requires continuous administration. PaaS enables the user to rent operating systems, hardware, storage and network capacity over the network. In the PaaS service model, the customer rents a set of toolkits to develop their own platform to deploy applications. PaaS providers give access to the different sets of software building blocks to create new applications. The customer has total access to upper layers and the application layer. Service providers control operating systems and hardware.

PaaS enables developers to upgrade and change operating system features. The main benefits of PaaS over traditional application development and deployment models are server and storage overhead, network bandwidth, software maintenance, support personnel and lower skill requirements. Any significant change in infrastructure increases the IT budget and requires workforce training, business process changes and more customer care. PaaS service models may not be a complete solution for every application within an enterprise. The platform standardization can bring more challenges and limitations in programming a new system to support automation and multi-tenancy features. PaaS may not be a good choice where an application needs customization for the underlying software or hardware.

In PaaS, configuration and settings files are critical and any modification or changes in the settings from an adversary can affect the entire cloud environment. As in SaaS, PaaS also has restrictions in controlling the underlying infrastructure. There is no access possible other than at the application and user control level. Network intrusion prevention is under the control of the cloud provider. Since PaaS is a Service Oriented Architecture, security issues related with SOA such as Man-in-the-middle attacks, DOS attacks, XML-related attacks, and injection attacks are the top security challenges. PaaS public APIs used to deliver management and user functionality should be secured with standard implementation and controls [27, 28].

4.3.2 PaaS Solutions

In PaaS, customers have full control of their applications and can log access information in a configurable way. One option for PaaS is to provide a central log server where customers can encrypt and sign log data and store log information in order to protect logs from possible eavesdropping or alteration [9]. With PaaS, the CSP can supply a log module to the end user so that they are able to store their own logs on the cloud. This can allow forensics to be performed without the participation of CSPs [13].

Encryption has traditionally been used to secure data residing on internal systems or to protect data in transit from one system to another. The cloud environment requires that data be encrypted internally within the CSP's environment, but is available to authorized end users as well. This requires an encryption technology that supports and extends cross-domain policies in a third-party environment, operates in real-time in a virtualized and multi-tenant environment while ensuring application functionality is not impaired, provides for enforcement of service-level controls defined by end user policies, and enforces segregation of duties at multiple tiers, and between end users and CSPs [29]. Traditionally, if cloud-hosted data is encrypted, basic server-side operations such as indexing, searching and sorting are impossible.

Homomorphic encryption is based on the idea that there are multiple ways to reach the identical mathematical outcome. This technology can be used to perform operations on ciphertext in a cloud environment and process encrypted data while still within an encrypted envelope, although this introduces an enormous increase in processing time due to key generation and the footprint of the ciphertext that expands in tandem with the number of keys [29]. One solution is to develop an encryption proxy that allows for both CSP data ownership and control, and server-side processing of encrypted data by leveraging bidirectional encryption and exposing a minimal amount of metadata to support server-side operations [29]. By encrypting data for the entire duration of its lifecycle (at rest, in transit, and in use) the data remains unreadable to third-party entities while being accessible to the end user and providing limited information for processing at the server [29].

Any issues related with SaaS are applicable to PaaS. According to Sandikkaya and Harmanci [28], Trusted Computing Base (TCB) should be secured and provide a standard API for users. Another solution is minimizing TCB to omit common coding mistakes. Before providing access control to the development platform, the vendor can implement a mechanism to verify the password more accurately by including additional security questions. In addition to the vendor security mechanism, the customer can analyze the operational standards of the CSP, including password complexity requirements and how they protect sensitive data. Moreover, an effective encryption scheme should be applied to the logon process by using a cryptographic hashing mechanism. Implementing a roles-based framework in authorization permissions at the application level ensures greater flexibility and secures permissions to different levels.

Network latency and round trip times are other issues found in PaaS or in any cloud environment. As latency is directly related with long distance, cloud latency becomes worse if the datacenter is located far away from the customer site. Optimizing the WAN and using load balancers to handle multiple requests can reduce cloud latency. Using Network Time Protocol or Clock Sampling Mutual Network Synchronization in the cloud environment will provide time synchronization. In order to report errors or exceptions of the application running in the cloud, a sufficient mechanism using message-based delivery should be implemented.

5. CURRENT PROJECTS

The European Network and Information Security Agency (ENISA) suggests that providing good security practices and clear SLA contracts can help to avoid legal problems [30]. In [31], the TCI architecture has been adopted by the Cloud Security Alliance (CSA) for cloud technology security and governance. This architecture combines frameworks such as the SPI model, COBIT, SOX, PCI, ISO 27002 and architectures such as SABSA, ITIL, and Jericho. These architectures define business operation support services, types of services, operation and support, and security and risk management. The National Institute of Standards and Technology (NIST) has published a taxonomy for cloud security that covers different roles involved with CSPs, cloud customers, cloud carriers, cloud brokers and cloud auditors.

CERT researchers Claycomb and Nicoll [32] discuss three different insiders involved with cloud-related threats: the rogue cloud provider administrator, the employee victim organization, and the insider who aims at internal attacks in an IT infrastructure. For rogue administrators, CSA suggests enforcing strict supply chain management, specifying human resource requirements, maintaining transparency over information security and management, and analyzing security breach notifications [8]. Shin et al [33, 34] have performed research on topics pertaining to authorization and access control.

Future areas of research may include providing standardized forensic services as Forensics-as-a-Service. According to Höner [35]. In coming years, improvements in existing research like nested authentication credential and stronger encryption algorithms are expected. There are many issues yet to be studied especially in secure virtualization. Designing forensics architecture for the cloud, extending current investigative tools into the cloud and creating effective legislation for cloud environment technology are three valuable future research directions in cloud forensics [10]. Other interesting research topics in cloud computing include: socio-technical approach to insider threats, predictive models, identifying cloud based indicators, awareness and reporting, policy integration, and normal user behavior analysis.

6. CONCLUSION

Cloud computing provides an easy, flexible and cost-effective IT solution for the ever changing requirements of today's enterprise. However, even with the tremendous benefits of cloud computing, many organizations are hesitant to embrace this technology due to security concerns. The increasing demand for cloud technology requires highly secured services to maintain the confidentiality, integrity and availability of data and computing resources. This paper has analyzed cloud security challenges and solutions from the perspective of IaaS, SaaS and PaaS services. Research into viable cloud security solutions is still in its infancy. Based on the analysis, it is recommended that CSPs take more steps to ensure cloud security by implementing advanced technologies to store log events and creating robust APIs that will be helpful for customers in maintaining a secure environment on both the provider and consumer ends of the spectrum. A forensics-enabled cloud will allow more customers to securely leverage the power of cloud computing services in the coming years.

7. ACKNOWLEDGMENTS

This research is supported by the National Science Foundation.

8. REFERENCES

[1] Market Research Media, 2012. Global cloud computing market forecast 2015-2020. Retrieved from: http://www.marketresearchmedia.com/2012/01/08/global-cloud-computing-market/

[2] Zawoad, S., and Hasan, R. 2013. *Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems*. Masters Thesis. University of Alabama at Birmingham Birmingham, Alabama.

[3] Talbot, Chris (May 1, 2014). Talkin' Cloud. Bitglass Report: Security Concerns Limit Cloud Adoption. Retrieved from: http://talkincloud.com/cloud-computing-research/050114/bitglass-report-security-concerns-limit-cloud-adoption

[4] Shetty, Sony. 2013. Gartner Says Cloud Computing Will Become the Bulk of New IT Spend by 2016. (October 2013) Retrieved December 12, 2013 from http://www.gartner.com/newsroom/id/2613015.

[5] D. Reilly, C. Wren, and T. Berry, "Cloud computing: Pros and cons for computer forensic investigations," *International*

Journal Multimedia and Image Processing (IJMIP), vol. 1, no. 1, pp. 26-34, 2011

[6] P. Mell, and T. Grance, "The NIST definition of cloud computing," 2011.

[7] Jackson, C., Agrawal R., Walker, J. & Grosky, W. 2014. Scenario-based Design for a cloud Forensics Portal. In *Proceedings of the IEEE International Symposium on Technologies for Homeland Security,* Waltham, MA, USA.

[8] Brodkin, J. (2008). Gartner: Seven cloud-computing security risks. *Infoworld*,*2008*, 1-3.

[9] Zawoad, S., Dutta, A. K., & Hasan, R. (2013, May). SecLaaS: secure logging-as-a-service for cloud forensics. In *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security* (pp. 219-230). ACM.

[10] Ruan, K., Baggili, I., Carthy, J., Kechadi, T. 2011. Survey on cloud forensics and critical criteria for cloud forensic capability: A preliminary analysis. ADFSL Conference on Digital Forensics, Security and Law.

[11] Paul, A., Anvekar, K, M., Rishil, J., and Chandra, S, K. 2012. *Cyber Forensics in Cloud Computing*. Master Thesis. Department of Computer Science and Engineering, NITK, Surathkal, India

[12] Birk, D. and Wegener, C. 2011. Technical Issues of Forensic Investigations in Cloud Computing Environments. *Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 IEEE Sixth International Workshop, (*May 2011), 26-26.

[13] Sang, T. (2013, January). A log based approach to make digital forensics easier on cloud computing. In *Intelligent System Design and Engineering Applications (ISDEA), 2013 Third International Conference on* (pp. 91-94). IEEE.

[14] Alvarado, M. D., Agrawal, R., & Baker, Y. (2013, April). Security mechanisms utilized in a secured cloud infrastructure. In *Southeastcon, 2013 Proceedings of IEEE* (pp. 1-5).

[15] Rai, R., Sahoo, G. and Mehfuz, S. "Securing Software as a Service Model of Cloud Computing: Issues and Solutions," *arXiv preprint arXiv:1309.2426*, 2013.

[16] Dykstra, J., & Sherman, A. T. (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. Digital Investigation, 9, S90-S98.

[17] Bouayad, A., Blilat, A., and Ghazi, M, E,. 2012. Cloud computing: Security challenges. 2012. *Information Science and Technology (CIST),* (Oct. 2012), 22-24.

[18] Subashini. S., and Kavitha, V. 2011. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications* 34.1 (2011): 1-11.

[19] Damshenas, M., Ali, D., Ramlan, M., and Shamsuddin, b. 2012. Forensics investigation challenges in cloud computing environments. *Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference,* (June.2012), 26-28.

[20] Dawoud, W., Takouna, I., and Meinel, C,. 2010. Infrastructure as a service security: Challenges and solutions. In *Informatics and Systems (INFOS),The 7th International Conference,*(2010), 1-8.

[21] Hay, B., Kara, N., and Matt, B. 2011. Storm Clouds Rising: Security Challenges for IaaS Cloud Computing. *System Sciences (HICSS), 2011 44th Hawaii International Conference on* , (7 Jan. 2011) 4-7.

[22] Birk, D. and Wegener, C. Technical issues of forensic investigations in cloud computing environments. *Systematic Approaches to Digital Forensic Engineering*, 2011.

[23] Dykstra, J. and Sherman, A. Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *DoD Cyber Crime Conference*, January 2012.

[24] Marty, R. Cloud application logging for forensics. In *In proceedings of the 2011 ACM Symposium on Applied Computing*, pages 178-184. ACM, 2011.

[25] Zafarullah, Z., Anwar, F. and Anwar, Z. Digital forensics for eucalyptus. In *Frontiers of Information Technology (FIT)*, pages 110-116. IEEE, 2011.

[26] Krautheim, F.J. "Private virtual infrastructure for cloud computing," In Proceedings of the 2009 conference on Hot topics in cloud computing (HotCloud'09). USENIX Association, Berkeley, CA, USA.

[27] Birk, D. and Wegener, C. 2011. Technical Issues of Forensic Investigations in Cloud Computing Environments. *Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 IEEE Sixth International Workshop, (*May 2011), 26-26.

[28] Sandikkaya, M, T., and Harmanzi, A, E,. 2012. Security Problems of Platform-as-a-Service (PaaS) Clouds and Practical Solutions to the Problems. *Reliable Distributed Systems* (SRDS), 2012 IEEE 31st Symposium on. IEEE, 2012.

[29] Vaultive Inc, 2014. Taking Control of Cloud Data: A Realistic Approach to Encryption of Cloud Data in Use. Retrieved from: http://www.vaultive.com/wp-content/uploads/2013/01/Taking-Control-of-Cloud-Data-A-Realistic-Approach-to-Encryption-of-Cloud-Data-in-Use.pdf

[30] Nelson, G., Charles, M., Fernado, R., Marcos, S., Tereza, C., Mats, N. and Makan, P. 2012. A quantitative analysis of current security concerns and solutions for cloud computing. *Journal of Cloud Computing 1.1* (2012): 1-18.

[31] CSA (2011) CSA TCI Reference Architecture. https://cloudsecurityalliance. org/wp-content/uploads/2011/11/TCI-Reference-Architecture-1.1.pdf

[32] Claycomb, W. R., and Nicoll, A. (2012, July). Insider Threats to Cloud Computing: Directions for New Research Challenges. *In Computer Software and Applications Conference (COMPSAC)*, (2012) 387-394.

[33] Shin,D., Akkan,H., Claycomb,W. and Kim,K. 2011. Toward role-based provisioning and access control for infrastructure as a service (IaaS). *Journal of Internet Services and Applications,* (2011), 243-255.

[34] Shin, D., Wang, Y., and Claycomb, W. 2012. A policy-based decentralized authorization management framework for cloud computing. In *Proceedings of the 27th Annual ACM Symposium on Applied Computing*, 465-470.

[35] Höner, P. 2013. Cloud Computing Security Requirements and Solutions: a Systematic Literature Review. Master's Thesis, University of Twente, 7500AE Enschede, The Netherlands.