Surveillance on Security Issues in Cloud Computing: A View on Forensic Perspective

DANLAMI GABI

Abstract— The rapid evolution of cloud computing over decade has drawn a wider attention to the number of subscribers growing over time as a result of the flexible services offered by cloud computing. Due to the cloud's flexible security architecture, attacks have occurred which emanate from subscribers' cloud-based infrastructure and are passed-through to the end users. It has become difficult to make general forensic diagnoses due to the differing (flexible) security architectures in use in the cloud. In this paper, we key our research on security issues in cloud computing, with a demonstrated experiment. During our experiment, we make use of virtual machine (VM) and set a window server 2003 operating system to serve as a forensic server that monitor and record the behavior of attacks emanate from the cloud and affect end-users of cloud subscription services. At the end of our experiment, we conducted a forensic investigation on this machine, which enables us to obtained ideal evidence.

Index Terms — Security; Privacy; Surveillance; Cloud Computing; Forensic Investigation.

1. OVERVIEW

IN the cloud, data security is the talk of the town as [enterprise level and user-level] privacy measures are required to ensure that vital information is not easily passed to the hands of criminals who would use the vital information for criminal purposes. With the advent of cloud computing, a vast range of applications ranging from social networking, web application hosting, and high performance computing have emerged [12]. According to "Yan [3], cloud computing, as being defined by the American regulatory body, National Institutes for Standard and Technology (NIST)", "…is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction." Cloud computing enables rapid changes to network operations, through provision of applications, platforms and also software support as a service (SaaS).

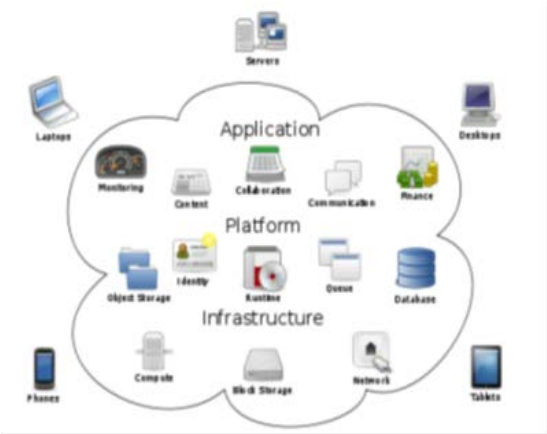


Fig. 1. Cloud Computing Environment [9].

The advent of cloud services enabled resource sharing at low cost and has made dynamic allocation of CPU, storage, and network bandwidth more flexible [15]. Due to its flexibility, as well as the number of subscribers, it is impossible to engineer a single security protocol to prevent malicious network attacks. Generally, for purposes of this paper, we refer to those who conduct malicious network attacks as "criminals" – we do not make any distinctions between those who originate malicious network attacks. We define malicious attackers as those who tend to violate the privacy of the [subscriber's] security implementation or who intend to evade the security policies of the [subscriber's] system, thereby carrying out their malicious activities. Security personnel at their own end [at the user-level] cannot actually eradicate the security vulnerabilities from the entire network architecture.

However, since the Internet serves as a communication infrastructure for cloud providers, which mandates the use of TCP/IP protocols, a hacker, be it an internal or external user is able to trace the IP address of a machine that they wish to compromise. In this instance, a malicious user can determine which physical server a legitimate user is using and eventually, implant a malicious server at his own end to launch an attack (Sabahi [7]. Because all of the users who use same virtual machine as infrastructure; if a hacker steals a virtual machine or takes control over it, he will then be able to access all users' data. The hacker can copy vital data into his local machine before the cloud provider could detect the action, meaning that virtual machine is out of control [7].

As resource pooling within the cloud makes it impossible to know the actual number of computers that are connected to the cloud services, forensic experts are beginning to emerge to determine how different network attacks happens with the use of forensic tools, which help investigate criminal activities and determine where these activities are coming from. "While Cloud Forensics is a field at its infancy stage, it is gaining relevance as growing number of companies look to leverage Cloud technologies to unlock the advantages from economies of scale and increased focus on their core strategic mission." [13]. To further describe the phenomena of cloud forensics, we cite researchers [4], citing [18], in which they state:

"Sin [18] highlighted in his proceedings on new digital forensic investigation model that, 'Computer Forensic is the use of scientifically derived and proven methods towards the Preservation, Collection, Validation, Identification, Analysis, Interpretation and presentation of digital Evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal or helping to anticipate the unauthorized actions shown to be disruptive to planned operations."

Therefore, using the preceding theory as our model, to further determine the course of this research, we set up a surveillance engine on a cloud-based service to determine the attacks that do emanate from cloud, with a practical experiment. At the end of our experiment, a forensic investigation was carried out on the surveillance engine and ideal evidence was discovered.

2 PRIVACY ISSUES IN CLOUD COMPUTING

This section describes the importance of privacy and sets out the relevance of our experiment to the emerging field of cloud forensics. Privacy is most important when it comes to the issue of business; because, it helps to ensure that personal data are protected from unauthorized collection, uses, and disclosure thereby preventing the loss of customer trust and inappropriate fraudulent activity such as theft of identity, email spamming, and phishing [15] p.149. "Data privacy in Cloud is the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal issues surrounding them [15] p.149." The problem of controlling what information one reveals about oneself over the internet, and who can access that vital information has prompt the users to ask the kind of privacy involved in cloud. Fig. 2, shows how a virtualized unsecure cloud computing service can be violated by an attacker whose aim is to intercept confidential informations belonging to company 'A'

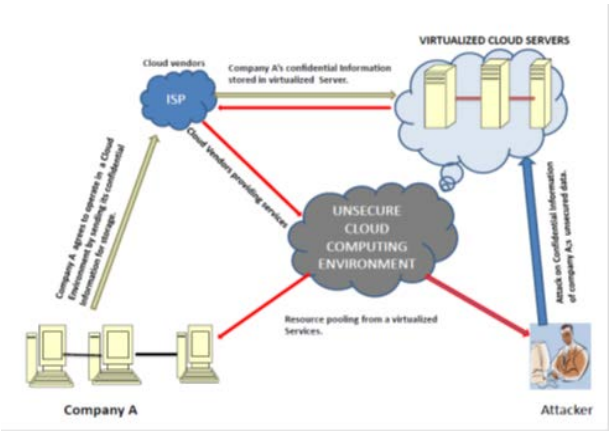


Fig. 2. How migration, resource pooling and attack takes place in Cloud .

The resultant flexibility of Cloud services has made protections of vital information still at its infancy stage. The trouble issues are how web sites which are visited collect, store, and possibly shares personally identifiable information about users [15]. Personally identifiable information (PII), as used in information security, refers to "information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual [15] p.154."

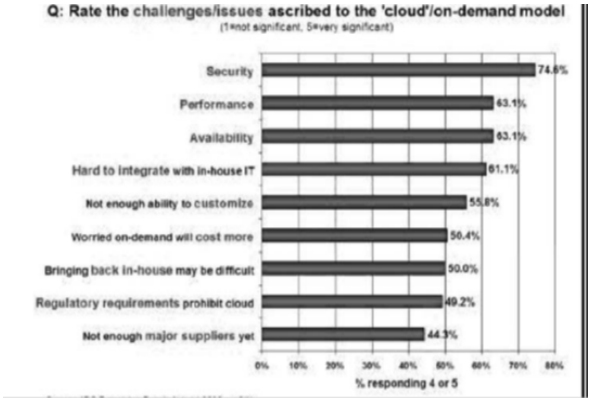
When vital information about a business, government agency, or other entity is disseminated in cloud, privacy or confidentiality questions may arise on how these informations can be protected in order to not to get to the hands of unauthorized users. "The location of information in the Cloud may have significant effects on the privacy and confidentiality protections of information and on the privacy obligations of those who process or store the information. Information in the Cloud may have more than one legal location at the same time, with differing legal consequences. Legal uncertainties make it difficult to assess the status of information in the Cloud as well as the privacy and confidentiality protections available to users [15] p.155." Having described the importance of privacy, we now turn to the major challenges faced in cloud computing when it comes to securing private data.

3 SECURITY CHALLENGIES IN CLOUD COMPUTTING

When dealing with private data in the cloud, security cannot be left alone. Security of data in conventional [physical, hardware-based] systems is handled by authentication, Access Control and Authorization principles. From the genesis of cloud, the cloud service providers such as, Third-party providers are increasingly providing storage and computational resources to their customers through services (Software as a Service, SaaS) such as Google Docs and Gmail, underlying platform (Platform as a Service, PaaS) such as Microsoft Azure, and underlying infrastructure (Infrastructure as a Service, IaaS) such as Amazon's Elastic Compute Cloud (EC2) [10]. "Rittinghouse and Ransome [15] p.157 explain:

SaaS is a model that involves the deployment of software to guarantee the use of applications that are license for user to use. PaaS is the base level development for SaaS where all the developed web applications are available for developers. It's also refers to as the "Cloudware" because of its working facilities for the designing of applications. IaaS is a platform virtualization environment that allows end users to access resources without minding the cost of maintenance or purchase of equipment rather; they buy the resources as fully outsourced service."

All of these services deployed by cloud service providers have enabled and engineered the migration of organizations to cloud. But still, there is a battle over security breaches in which many questions [are] unanswered by the service providers. Fig. 3 below shows a statistical percentage of [how] high risk security breach can be when operating cloud services.



Source: IDC Enterprise panel (2010)

Fig. 3. Result of IDC [International Data Corporation] ranking security challenges in Cloud Computing.

Lack of security is not the only hurdle in wide adoption of cloud computing. Cloud computing is surrounded by many security issues like securing data, and examining the utilization of cloud by the cloud computing vendors [1]. Additionally, per [6], individual end-users may no longer be able to control or deploy their own investigations into security incidents emanating from the cloud. They write:

Security policies, companies' main pillar concerning security, cannot be easily deployed into distributed, virtualized cloud environments. This situation is further complicated by the unknown physical location of the companies' assets. Normally, if a security incident occurs, the corporate security team wants to be able to perform their own investigation without dependency on third parties. In the cloud, this is not possible anymore: The CSP obtains all the power over the environment and thus controls the sources of evidence. In the best case, a trusted third party acts as a trustee and guarantees for the trustworthiness of the CSP (p. 3).

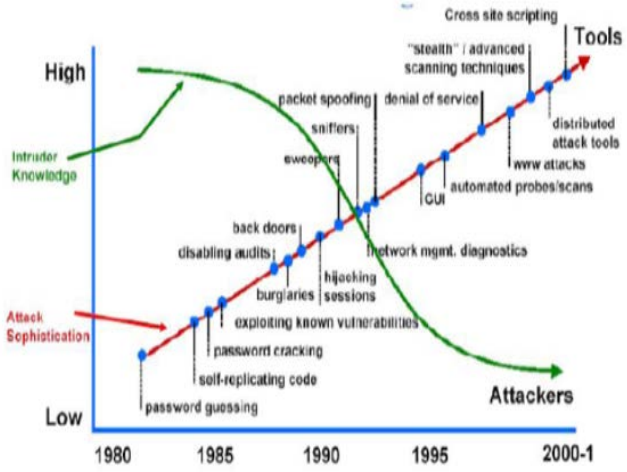


Fig. 4. Intruder's Technical knowledge Against Sophistication Attacks and Tools [8].

Fig. 4, shows a straight graph presenting forms of attack that do emanate in the cloud computing architecture. The curve line within the graph, indicate the high level of attacks that takes place as being confronted by the attackers in their yearly sequence.

Since security issues is the main threat to cloud computing, it is vital to come out with a lasting solution in securing vital information, a solution that can prevents vital information from getting to the hands of illegitimate users. In ensuring that this occurs, both the cloud service providers and the third parties providers most work at each end in ensuring maximum security implementation, so as to prevent unauthorized access and ensuring business continuity.

4 FORENSIC ISSUES IN CLOUD COMPUTING

It is however, easier said than done. With the advent of cloud computing, investigation within the cloud is impossible due to inter-boundary covered by cloud service. But however, according to et al., "Cloud computing brings opportunities for cloud forensics tracing Internet criminals in the distributed environment. Cloud forensics also involves complicated crime-scene investigations." But, interpreting these concepts in the context of cloud computing service, widen the scope towards how investigation can be carry out in cloud computing environment. The vast service of cloud computing brings investigation at still, looking at inter-boundaries jurisdictions which made search for evidence more difficult. However, with the idea of IP tracing, forensic expert can narrow down their search to track down perpetrators of cloud service.

Because cloud base system uses IP address to identify each others when communicating, attack on IP address is easily spoofed with systems that use cloud services. Looking at these issues, tracing a system where such attacks came from is one of the applications of Forensic expert in their dealings with security issues. The concept of traceback was looked at by [14] in their preceding on Network Security where they stated that, "the purpose of IP traceback is to identify the true IP address of a host originating attack packets which is done by checking the source IP address field of an IP packet. Because, a sender can easily forge this information, however, it can hide its identity." These justification was looked into the proposed model on cloud traceback by Waheed [11] as shown in fig. 5, where they elaborated that; the proposed traceback model can be place at the cloud system infrastructure, which contain a mark tag within the cloud traceback header, that marks all incoming request so as to prevent attack. This model hides the server address and at the same time identify request source.

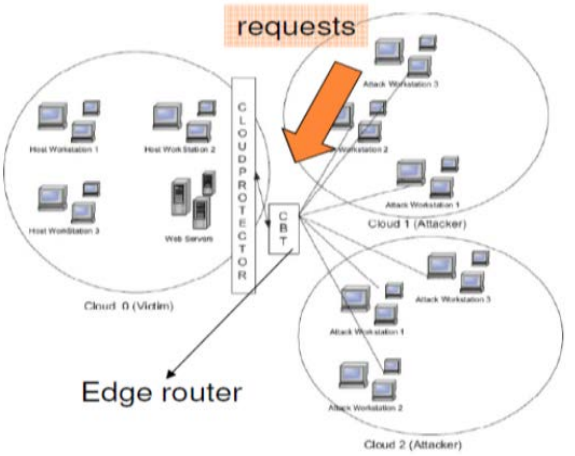


Fig. 5. Cloud TraceBack within cloud system infrastructure [11].

"The main drawback of cloud computing from a forensic perspective is that of data acquisition-knowing exactly where the data is and actually acquiring the data. The search and seizure procedures used in the conventional computer forensic process are impractical due to evidence being stored in cloud datacenters. It is also difficult if not possible to maintain a chain of custody relating to the acquisition of the evidence [5]." But we asked, how can we deploy a standard forensic procedure to cloud investigation? To answer our question, in our research, section 6 is an experiment we conducted on cloud base system. After the experiment, a live forensic investigation was carried on the Machine that serves as a forensic server through the application of live analysis as one of the steps adapted by forensic experts in the discovery of evidence.

5 DATA ENCRYPTION A CONCERN ISSUES IN CLOUD COMPUTING

Before we describe our experiment, it is important to discuss encryption within the cloud. Encryption as viewed in cloud is a greater concern as its interpretation depends upon the possibility of its implementation. The migration of confidential data to cloud and its hostage on distributed or virtualized servers that can be accessed from different central locations can be look into, until a means on how security of data is guaranteed. Considering the flexible computing architecture of cloud, implementing encryption will violate the aim of the service provided. This is because, the initial idea of making cloud computing a user friendly service is to allow end-users have [an] easy access service in form of pay-as-you go without restriction and minding what services [SaaS, IaaS and PaaS] to maintain.

"Stallings and Brown [16] p.43 were able to defined encryption as:

…..the process of translating plaintext into ciphertext using a secret key with a cryptographic cipher (algorithm)."

Data encryptions provide confidentiality [data transmitted over a secure channel], integrity [data transmitted without interception by third party] and availability [data able to reach to its destination]. Encrypting data in a distributed or virtualized server will be a difficult task and can lead to restriction of access if properly implemented. That is, it can provide some form of restriction to service availability thereby turning down its aim of being a flexible architecture. This is because; a service that is meant to provide easy access will now become a restricted service. If encryption is properly implemented, it will guarantee protection to data in a virtualized server, provided it will not deny any end-user access to resources. Security of data in cloud encourages company and corporate organizations to migrate to cloud computing service; it will expand the operation of the cloud architecture with a reliable entrusted computing environment that creates [bring to existence] unlimited network expansion. The drawback of this implementation is the level of its virtualization. We cite the statement of [6], on the possibility of implementing security in a virtualized cloud environment and they said:

"…..Security policies, companies' main pillar concerning security, cannot be easily deployed into distributed, virtualized cloud environments. This situation is further complicated by the unknown physical location of the companies' assets….."

Reviewing these statements, it is clear that, virtualized cloud environment are very difficult to implement encryption due to multiple servers situated at different location performing different functions all together. Looking at unencrypted architecture of cloud computing and the zero level of security implementation, we will experiment vulnerably how cloud computing architecture is with the use of forensic server and later discover evidence that are forensically examined.

6 EXPERIMENTS

In our experiment, we seek to prove or disprove our question by creating a scenario that will elicit data which tells us that cloud computing service is not well secure to store confidential data. The experiment conducted was monitored for three consecutive days. In this section, we set out how we set up our data-capture [forensic server]. The data capture is set up using a virtual machine [VM] containing a Window 2003 operating system config.d to serve as a forensic server. At a later time, this capture device is meant to convey different forms of attacks emanating from the cloud architecture and store evidence of these attacks. The essence of this experiment is to disguise the attacker to see the forensic server as a virtualized server.

The forensic server is set on wireless cloud service architecture and an IP address is assigned using DHCP. In determining the IP address of the server, the DOS command, of the operating system was lunched using **'start-run-cmd'**. At the DOS command prompt, we typed **ipconfig/all**. This enables us to discover the IP address automatically assigned to the forensic server. A ping request was tested using a different machine towards the forensic server and a successful echo-reply was achieved. In view of this, we ensure that no interference what so ever to disrupt network access to the surveillance

engine [forensic server]. Fig. 6 is an experimental setup for the surveillance engine.

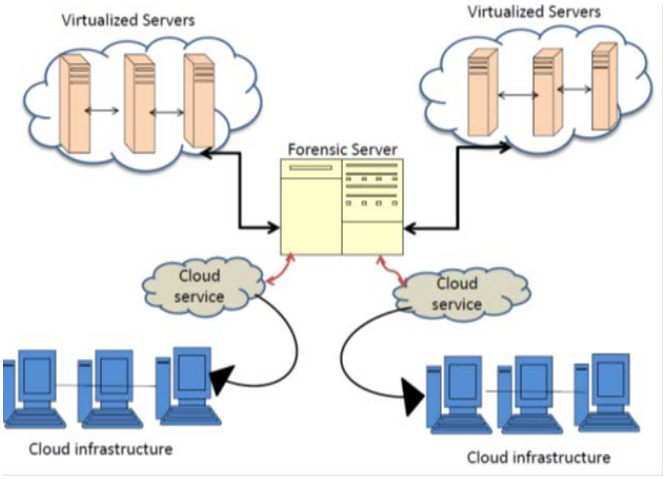


Fig. 6. Cloud computing architecture setup for attacks discovery.

Within the forensic server, we ensure that the firewall is turn-off so as to allow the passage of any form of attack for recording purposes and also set an intrusion prevention system [IPS] within the forensic server to prevent passage of such attacks to the virtualized server. After we successfully concluded the experiment for three consecutive days, the forensic server was later examined and the following forms of attacks from the first day to the third day were discovered:

TABLE 1
ATTACKS GATHERED FROM THE FORENSIC SERVER AFTER SUCCESSFUL EXPERIMENT ON CLOUD INFRASTRUCTURE

DAY / INCIDENCE	ATTACK TYPE	NO. OF ATTEMPTS	SUCCESS RATE
DAY 1	Password guessing	3	Fail due to strong password encryption on the forensic server.
	XML message	2	Message flooded with XML message instead of packet but fail to disrupt network access.
	DDOS	1	Server monitored an attack from several systems and immediately reboot.
DAY 2	Packet sniffing	5	Successfully due to lack of encryption.
	Packet spoofing	2	Spoofing successfully executed by the attacker.
	XML message	4	Message flooded with XML message instead of packet but fail to disrupt network access
DAY 3	Cross site scripting [XSS]	2	Server monitored script execution through session hijacking
	Scanning attack	4	Successful, forensic server trace IP scanner and store evidence.
	DDOS	3	Server monitored an attack from several systems and immediately reboot.
	Hacking	2	Forensic server noticed unauthorized request using metasploite tool and the system was rebooted.

We carried out a live forensic analysis in discovering traces of attacks and the evidence they left behind as discuss in section 7.

7 FORENSIC EVALUATION OF THE SURVEILLANCE ENGINE [FORENSIC SERVER] FOR TRACE OF EVIDENCE

Acquisition of evidence on cloud servers is an ambiguous task; as the volume of data that are said to be situated, including the capacity of the storage media has made forensic search mealy impossible. The conclusion of our experiment with the use of forensic server as a data-capture enable us investigate the forms of attacks that made cloud computing architecture not secure to store confidential data. Section 6, table 1 are the evidence of attacks that resulted from the forensic server after examination. In other to trace password guessing on the forensic server, we lunched the registry editor [HK_LOCAL_MACHINE] of the forensic server and cross-examine it. We discovered that a password guessing tool: EssentialNet was found on the server, specifying the version, the website where such tool was downloaded as shown on fig. 7. This tool is use to perform sniffing and spoofing attacks as there are many exploit which can be used from the tool such as IP scanning.

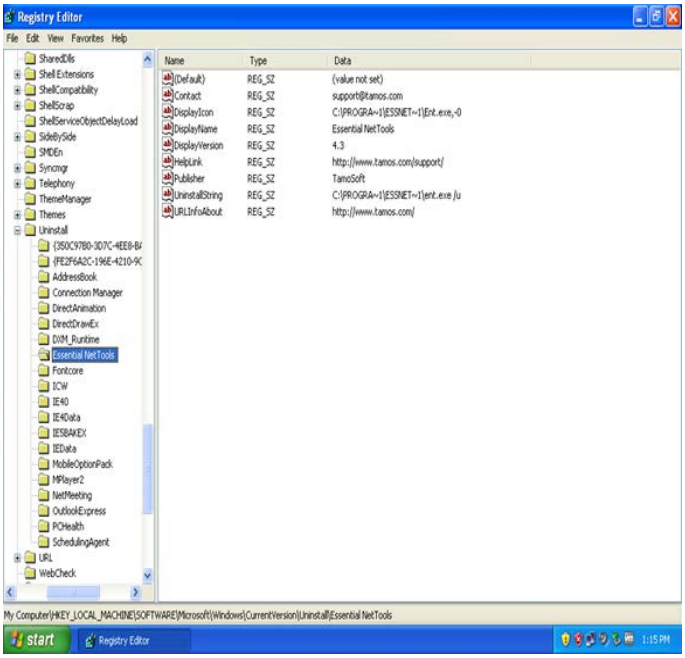


Fig. 7. Evidence of EssentialNet tool in compromising password (Gabi 2014)

The event log of the forensic server experimented was said to have kept all the attack evidence that took place. It was discovered that, an anonymous user have accessed the server using a metasploite penetration testing tools trying to compromised the server, the server noticed a session establishment with the following retrieved code:

```
[*] Connecting to the server...
[*] Started bind handler
[*] Authenticating to 192.168.64.129:445|WORKGROUP as user 'administrator'...
[*] Uploading payload...
[*] Created \cCTleffh.exe...
[*] Binding to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.64.129[\svcctl] ...
[*] Bound to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.64.129[\svcctl] ...
[*] Obtaining a service manager handle...
[*] Creating a new service (WvRVpDWv - "MHBlsLIj22KhyAhEauDjbyjcECEAz")...
[*] Closing service handle...
```

Fig. **8:** Evidence showing two-way handshake between the forensic server and the system that initiate attack using metasploite tool.

In our search for evidence, we also discovered that, the Window registry of the server has some vital evidence about the computer that initiated the hacking attack. An IP address 192.168……. was found on the forensic server which was used to initiate session between the server. We also discovered that, attack with metasploite can compromised a server and also led to session hijacking where the attacker can make use of vulnerability available on the server and exploit account. During a successful attack, the hacker can deprive the administrator having access to the server by compromising the server password and changing it to his own logging account. Several attacks can still be found apart from the aforementioned attacks discovered in table 1.

The purpose is that, every cloud services originate from a Service provider. In terms of attack, the presence of these forensic server is meant to monitor the movement of request that are sent to cloud servers (E-mail, database or Web servers) and retrieve suspicious request to itself by purporting as the real server. And this forensic server will immediately send a message to the network administrator that, a suspicious message from Country A, with date and time of the message, the kind of message with the site from which the message originated from. In view of this, every suspicious message is diverted to the forensic server without granting it requests. We noted that, the deployment of this forensic server will help the network security personnel or information Security personnel, on how to think about what security measures should be put in place to counter any form of violation on data and unauthorized access through provision of security measures that will help elevate security breach.

The yearning of consumers towards cloud service providers [to provide secure services], is its inability to protect confidential information. Today, private sectors and commercial organizations with the inclusion of financial organization find it impossible to associate themselves with public cloud; but tend to develop their own private cloud through creating secured channels that will help ensure their data is well secured from both internal and external threats. The experiment at session 6, tends to discover several of the security challenge; attacks on data by hackers. However, information as it route across an unsecured channel via public services are easily intercepted by individuals who tend to violate the confidentiality of information. Data situated within the public cloud servers has low level of security as they can easily be accessed. Lack of encryption is a major and tedious problems confronting information in cloud. Cloud vendors cloud not guarantees the security of data as it route the net. In our experiment, evidence of attacks [as trace on the forensic server] provides a clear proof about the confronting challenges on data privacy when it comes to the issue of cloud.

8 CONCLUSION

Since the Cloud provides a flexible comfortable service through a virtualized delivery of data in our time, it is confronted with many security challenges that cannot be entrusted to store confidential data. In this research, we discovered the attacks confronting Cloud computing with an evidential view on forensic perspective. Because, security is still the defining process in Cloud, it is vital to find lasting solution to prevent breach of Confidential Information.

However, in our experiment, we demonstrated the use of forensic server [data-capture] in detecting and reporting threads that may result from the subscriber's infrastructures. The experiment provided us with a trace of evidence of Metasploite Tool and Essential Net tool as highlighted in session, which are tools that the attackers use in exploiting account.

Our discovery for evidence shows that, data privacy is

not guaranteed when it comes to the issue of Cloud. However, encryption is not taken into consideration by Cloud service providers and these makes it difficult for private firms and other agencies migrating to Cloud.

Our analysis also shows the way forward on security issues in Cloud computing; through implementation of standard encryption to data that need to be situated on Cloud Servers and also the deployment of Forensic servers at every location of the ISP's in detecting, and keeping track of unauthorized access.

9 RECOMMENDATION

In our research, we are yet to address the legal issues of Interboundary forensics and how imaging of the forensic Server is to be carried out. Our further research will look at this tec nique in other to unveil more forensic evidence.

REFERENCES

[1] B.F.Shaikh and S.Haider, "Security Threats in Cloud Computing," *Proc. Of The 6th International Conference on Internet Technology and Secured Transaction,* pp.214-219, Dec. 2011.

[2] C.Kaufman, R.Perlman, and M.Speciner, Network Security: *Private Communication in a Public World*. USA.: Prentice hall ptr, pp.215-219, 2002.

[3] C.Yan, (2011) "Cyber Crime Forensic System in Cloud Computing," *Proc. of the 2011 International Conference on Image Analysis and Signal Processin,* pp. 1-4, Oct. 2011.

[4] D.Gabi and A.Al-Nemrat, "Password Guessing Attacks: Analysis and Discovery of Evidence in Computer Forensic Investigation," *Proc. of 2012 2nd International Conference on Cybercrime, Security and Digital Forensic (Cyfo – 12),* S.R.G. Weir and A.Al-Nemrat, eds., pp. 53-72, May 2012.

[5] D.Reilly, C.Wren, and T.Berry, "Cloud Computing: Forensic Challenges for Law Enforcement," *Proc.of the Third International Conference on Multimedia Information Networking and Security,* pp. 1-7, Nov. 2011.

[6] D.Birk and C.Wegener, "Technical Issues of Forensic Investigations in Cloud Computing Environments," *Proc. of The Sixth International Workshop on Systematic Approaches to Digital Forensic Engineering Held in Conjunction with The 32nd IEEE Symposium on Security and Privacy,* pp. 1-10, May 2011.

[7] F.Sabahi, "Cloud Computing Security Threats and Responses," *Proc.of the International Conference on Internet Technology and Secured Transactions,* pp.245-249, Dec. 2011.

[8] I.Gul and M.Hussain, "Distributed Cloud Intrusion Detection Model" Vol.34, no.8, pp.71-82, available at: http://www.sersc.org/journals/IJAST/vol34/8.pdf Sept. 2011.

[9] K.P.Shelke, S.Sontakke, and A.D.Gawande, "Intrusion Detection System for the Cloud" Vol.1, no.4, pp. 67-71, available at: http://www.ijstr.org/final-print/may2012/Intrusion-detection-system-for-cloud-computing.pdf, Sept. 2012.

[10] M.Kantarcioglu, A.Bensoussan, and S.Hoe, (2011) "Impact of Security Risks on Cloud Computing Adoption," *Proc. of the Forty-Ninth Annual Allerton Conference on Communications, Control, and Computing,* pp. 670-674, Sept. 2011.

[11] N.Waheed, "Attack on Cloud Computing", pp. 1-35, available at: http://people.scs.carleton.ca/~maheshwa/courses/4109/cloud-attacks.pdf , 2013.

[12] S.Ahmed and A.Y.M. Raji, "Tackling Cloud Security Issues and Forensic Model," *Proc. of the 7th International Symposium on High Capacity Optical Networks and Enabling Technologies,* pp.190-195, Dec. 2010.

[13] S.Thorpe, T.Grandison, and I.Ray, "Cloud Computing Log Evidence Forensic Examination Analysis," *Proc. Of The 2012 2nd International Conference on Cybercrime, Security and Digital Forensic (Cyfo – 12),* S.R.G.Weir, and A.Al-Nemrat, eds., pp. 53-72, May 2012.

[14] T.Baba and S.Matsuda, "Tracing Network Attacks to their Sources," *Proc on Network Security,* pp. 20-26, March – April 2002.

[15] W.J.Rittinghouse and F.J.Ransome, *Cloud Computing: Implementation, Management and Security*. U.S.A.: Taylor and Francis Group LLC, pp.153-167, 2010.

[16] W.Stallings and L.Brown, Computer Security: *Principles and Practice*. New Jessy, USA.: Person Education, Inc, pp. 42-45, 2008.

[17] X.Fu, Z.ling, W. Yu, and J.Luo, "Cyber Crime Scene Investigations (C2SI) through Cloud Computing," In: *2010 International Conference On Distributed Computing Systems Workshops,* pp. 26-31, June 2010.

[18] Y.Shin, "New Digital Forensic Investigation Procedure Model," *Proc. Of The Fourth International Conference on Network Computer and Advance Information Management,* J.Kim, D.Delen, P. Jinsoo, F.Ko, and Y.Jin Na, eds., pp. 528-531, May 2008.

- *DANLAMI GABI is a lecturer at the Department of Computer and Information Technology, Kebbi State University of Science and Technology, Aliero, Nigeria. He is an MSC holder in Information Security and Computer Forensics from the Unniversity of East London, UK. E-mail: gabsonley4life@yahoo.ca*