Digital Forensics Model for Mobile VoIP Cloud Computing Investigation

Joshua Edward Mamza, Ismaila Idris
Cyber Security Science Department, Federal University of Technology, Minna, Nigeria.
joshua.pg6759@st.futminna.edu.ng, ismi.idris@futminna.edu.ng

ABSTRACT—Voice over IP on Mobile Cloud Computing (mVoIPcc) is gaining acceptance as a technology for transmitting voice or video data over IP based cloud networks. This can be attributed to the ability to rapidly develop and deploy VoIP application by mobile application developers and the free billing features of VoIP in correlation to the traditional circuit switch network. This creates two precarious precedents, first of which is attack associated with vulnerability on VoIP protocols such as call management protocols (SIP) and Media Delivery Protocols (RTP). Secondly is the forensics analysis challenge to investigators due to the converged attribute of mVoIPcc communications which are not bounded to any physical location. The latter is further complicated by Cloud Service Providers (CSPs) reluctance to provide vital digital forensics data within the CSPs internal networks. This paper reveals VoIP Digital Forensics Models (f VoIP-DEFSOP and VoIP-NFDE) for detecting, reconstructing and investigating compromised VoIP systems. A hybrid cloud forensics investigation model, which consist of Forensic-as-a-Service provided by the CSPs, and investigation model that can be adapted to cloud forensics called mVoIPc-IM.

KEYWORDS – CloudService Provider, Protocols, VoIP, Forensics Analysis Models, Mobile Cloud Computing

INTRODUCTION

Voice over Internet Protocol (VoIP) calls is common in existing telecommunications modus with bright potentials as the next century generational telephone of choice or preferred. The prodigious increase in the use of VoIP application has advanced the increased research by academia and telecommunication companies or Network Service Providers (NSP). This is not in part because of the growing acceptance of VoIP application, the benefits of using this kind of technology include but not limited to low call cost for locals, long distance and international. Most people now usually use telephone calls with IP mobile devices such as (WhatsApp calls, Facebook Video Calls, Skype, Imo etc) which synchronizes speech and video data to be transmitted over a long distance with data packets. . The cost is reduced drastically with the arrival of Mobile Cloud Computing (MCC). Mobile Clouding Computing allows mobile application to be deployed on the cloud, such applications can then be accessed on multiple platforms [1]. Mobile VoIP over Cloud (mVoIPc) enables VoIP Application operates in a virtualized environment independent of the mobile devices. Using APIs on mobile devices, users connect to the virtualized VoIP services in the cloud across multiple platforms via IP networks. The proliferation VoIP applications over the cloud on multiple mobile operating systems is an exemplification of how the two technologies (VoIP & cloud computing) have completely revolutionized how users communicate [2] over IP based network.

Detecting attacks or misuse of VoIP application requires the use Network Forensics Analysis Tools (NFAT). The tools uses network traffic and log files from other network applications such as IDS and firewalls to detect and reconstruct attacks [3]. Investigating attacks or misuse of mVoIPc using current NFAT is next to impossible due to the privacy concerns from the Cloud Service Providers (CSPs). The privacy concerns leave forensics investigators restricted to only log files from the compromised mobile devices and access points and mobile base stations used by the mobile device. This is because there is little or no access to the CSPs internal networks infrastructure where vital forensic evidence that will assist in reconstruction of attacks is located. The growth of mVoIPc has created a wealth of research in to different areas of mVoIPc, one such area is forensic pattern analysis. As of the time of writing of the paper, there is no unified research paper that has exam forensic pattern analysis in respect to mVoIPc.

This paper aim to address these by critically review and analyze security architecture, threats, vulnerability and current forensics investigation models of detecting, reconstructing and investigating VoIP attacks over Mobile cloud computing. Section 2 provides overview into VoIP, Mobile Cloud Computing and implementing VoIP over Mobile Cloud Computing. Section 3 takes a critically reviews at current VoIP Forensics Model and Patterns Analysis Frameworks, we also review current forensic evidence detection and reconstruction models. Section 4 we proposed mVoIPc forensics model for investigating VoIP attacks over cloud. Lastly is the conclusion in Section 5

OVERVIEW

Voice over IP is a technology that allows communication over broadband internet. Using IP networks, VoIP allows voice and video packet to be transmitted over public network such as the internet instead of the traditional fixed or mobile telephony. VoIP can be use to make audio or video calls between two points that is the source terminal and the destination terminal, which can be personal computer workstations, VoIP phones, mobile devices or two or more traditional phones provided they are connected to an IP network. The cost for user or an actor is neglibale compared to the use of VoIP applications is rapidly changing how users communicate universally. VoIP can be used for both business and domestic purpose. The emergency of MCC has greatly increased the proliferation of VoIP applications on mobile platforms. Operating in client-server architecture, MCC allows VoIP users connect to VoIP server installed virtually on the cloud. Using an APIs installed on mobile devices, VoIP phones, Computers, calls are initiated which is then routed through the cloud server to the destination user. In these section we critically examine current SIP based VoIP architecture, we also exam MCC and implementation of VoIP on MCC.

A. Voice over IP Architecture

The traditional phones system is based on copper wires carrying analog voice data over the dedicated circuits. Calls are transmitted over a dedicated channel between two points for the duration of the call. In SIP based VoIP, analog voice packets are converted into to digital voice packet using voice codecs. User calls are initiated and authenticated using Signaling Protocols (SIP) and Media Transfer Protocols such as Real-Time Transport Protocol (RTP) are used to transmit digitized voice packets over IP network. In SIP based VoIP consist of different component which includes User Agents and Proxy Server. SIP supported VoIP architecture uses proxy servers for call routing. The proxy server provides security mechanism for the terminal or mobile devices such as Authorization, Authentication and Accountability [4]. Below shows a hybrid VoIP SIP based architecture.

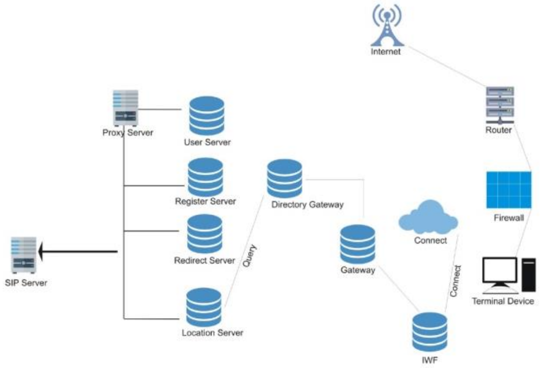

Fig. 1. Hybrid VoIP Signaling Protocol Architecture

The SIP User Agents (UAs) represents the phone and there are two parts to UAs: client and server, the client portion is called the User Agents Client (UAC) while the server portion is called the User Agent Service (UAS) [5]. The Register Server receives registration and requests update of Location Server which keeps track of UAs. The UAC is responsible for initiating a call by sending a URL-Addressed INVITE to the intended recipient UAC, while UAs receives the request and send back responses [6]. The proxy server is connected to a VoIP gateway and other proxy servers. In most cases the Location and Register Server are integrated into the Proxy Server. The Redirect Server functions as a router, it receives request, determines the next-hop server and return’s the address of the next-t-hop server to the client instead of forwarding the request.

B. Mobile Cloud Computing (MCC) Architecture

Cloud computing also refer to as grid computing or virtualization is exemplify by [7] as a model of convenient, on-demand network access to computing resources such as network, servers, storage, applications, and services that can be rapidly deployed with little management by CSPs. Based on the IT resource been provided, cloud computing are classified into three (3) category which are Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS). Cloud computing has completely transform how users consume IT across different platforms, one field cloud computing has transformed user IT usage is Mobile Cloud Computing (MCC). This is fast emerging as one of most exceptional branch of cloud computing and is expected to broaden the mobile eco system. [8]. MCC can be described as an on-Demand model of access IT resource over mobile networks. MCC enable applications operate autonomous of the mobile device by mitigating device data, processing power and storage. As a result mobile applications are rapidly developed and deployed with minimal efforts or CSPs reciprocal action. Using APIs on the mobile device, the mobile device send service request to the cloud server via access points, the cloud server allocates resources to the received request to establish connection [9]. Figure 2 shows an example of MCC architecture.

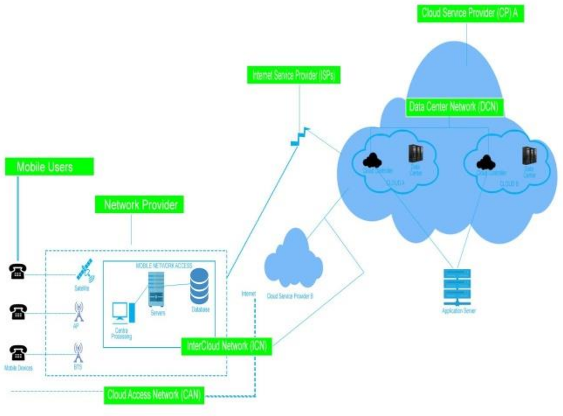

Fig. 2. Architectures of Mobile Cloud Computing

As seen on Figure 1, MCC architecture consist of mobile devices, mobile networks service (BTS and Access Point) provided by the mobile operator, the internet access provided by the Internet Service Provider (ISP) and lastly the CSPs infrastructure which contains the application server, Cloud Controller and the Cloud Data

Center. The critical elements interconnecting the various MCC architecture is the networking. As shown in Figure 2, we divided the network into three (3) segments, which are Cloud Access Network (CAN), Data Center Network (DCN) and Intercloud Network (ICN) [10].

CAN enable mobile device user's access to the cloud network, the segment consist of the wireless access point and satellites, it also consist of central processing, home agent and security (Authorization, Authentication and Accountability) servers which is provided by the mobile network operator. The DCN enables clusters of computers or application server interconnects with each other, in a sense DCN allows data center to data center intercommunication. The Application servers are located in these network segment include cloud controllers. The ICN enables two cloud infrastructure communicate with each other. Similar to DCN, it is located and controlled by the CSPs [10]

C. Architecture of Mobile Cloud based Voice over IP

Migrating storage space and computing power to the cloud service provider sees Mobile Cloud Computing (MCC) applications gaining popularity across the global. One such application that is retrieving due to the emergency of MCC is VoIP. The early VoIP system mirrors the architecture of legacy telephone network system and other VoIP system such as skype are based on closed private p2p secure networks. Depending how VoIP is implemented on MCC, VoIP services can be offered to user as Platforms as a Service (Paas) and Software as a Services (SaaS). Figure 3 shows the deployment of mVoIPc over Cloud Computing.

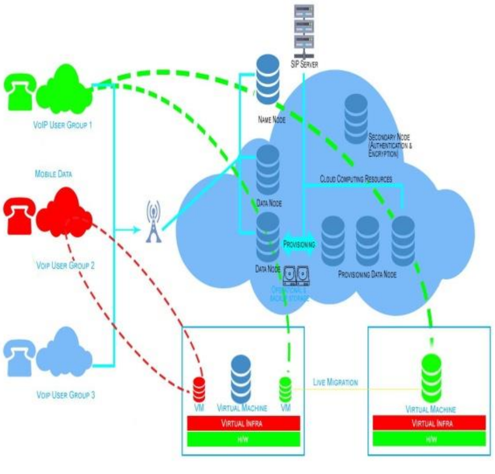

Fig. 3. Architecture Mobile Cloud based Voice over IP

In MCC based mVoIPc, the SIP proxy, Registration Servers are installed and configured on the CSPs servers. Using heterogeneous networks (wireless network, mobile network operators) Users access the VoIP cloud on smartphones, personal computers and other devices with internet access.

VOIP FORENSICS MODEL AND PATTERNS ANALYSIS FRAMEWORKS

The openness nature of VoIP protocols (SIP and H.323) and the inherit vulnerability associated with IP based real-time services such as VoIP permits such systems susceptibility to attacks by malicious users. Identifying, collecting, preserving and analyzing legal digital evidence is the primary aim of Network Forensics. In VoIP forensics, network patterns are used to analyze voice packet based on collected VoIP network traffic [11]. These method helps investigator to identify, detects, trace, investigate and determine attack point of origin and attack behavior [12]. Detecting VoIP digital evidence requires comparing normal and abnormal VoIP network traffic, when insufficient information for investigation is lacking, VoIP model employs the use Secure Temporal logic of action (S-TLA). S-TLA enable VoIP forensics model reconstruct digital evidence where lack of sufficient information about an attack is not available [13] [14]. This model also provides reliability and integrity for the collected information, validates the authenticity of the provided evidence, and allows NFIs to capture unknown attacks undetected by other network forensics methods [10]. In this section, we critically review current VoIP forensics analysis models and we review current network traffic capturing techniques used during VoIP forensics.

Current Network Forensics on wired and wireless networks can rapidly access compromised networks and network devices, but reverse is the case when investigating similar attacks on system over MCC [15]. This is because Network Forensics Investigators (NFI) restricted access to the internal networks and other resources of the CSPs, these in turn complicate acquisitions of forensics data and other critical forensics investigation procedure such as Access to Artifact and Chain of Custody respectively.

Another area of concern is user data privacy on the cloud, such as alteration of data by unauthorized users on the cloud, privacy of user data during forensics investigations' and integrity of user data during migrating between cloud networks. In this section, we take a critically look at current forensic mode and pattern analysis framework, in relation to detecting, collecting, examine and analyzing digital evidence at different segments of MCC (CAN, DCN and ICN) network [10]

Table I. VoIP Forensic and Pattern Analysis Framework

VOIP FORENSIC MODEL	
VOIP FORENSIC MODEL & PATTERN ANALYSIS FRAMEWORKS	
1	VoIP Network Forensic Digital Evidence (VoIP-NFDE)

2	VoIP Digital Evidence Forensics Standard Operating Procedure (VoIP -DEFSOP)

As seen from the Table I current VoIP network forensics model and pattern analysis frameworks. We grouped the models into two namely VoIP Forensics model and VoIP forensic pattern analysis frameworks.

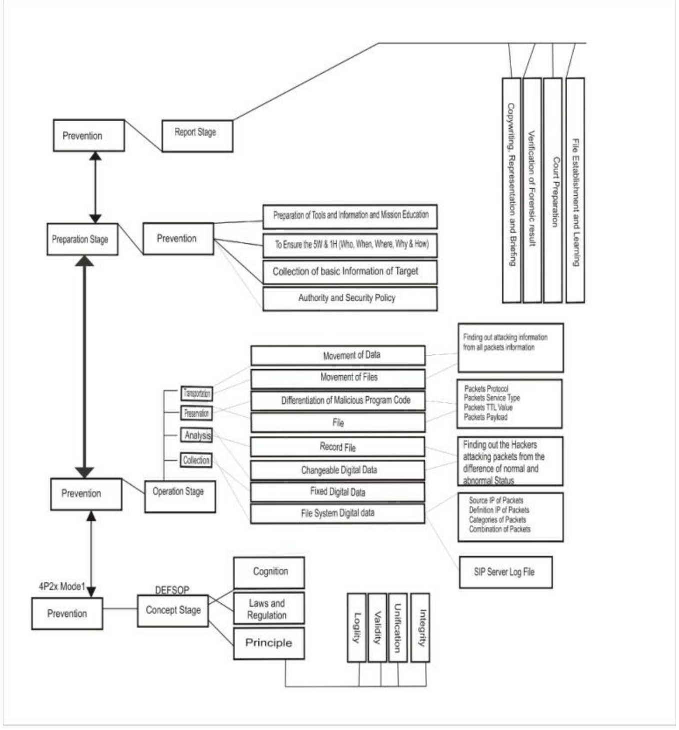

Fig. 4. DEFSOP Model

The first responders must exercise with caution when they seize any electronic device. The second stage is the Preparation Stage; the stage involves preparations before forensics investigation in order to prepare for the Operational stage of the VoIP-DFESOP. The preparation stage involves having basic information about the crime scene, preparing forensics tools needed, identifying forensic team members and a proper briefing relating to the crime scene. The third stage is the Operation Stage; this is the most important state on the VoIP-DEFSOP. It deals with the precaution taken in collection, preservation and transporting of digital evidence. More

A. VoIP Network Forensic Digital Evidence (VoIP-NFDE)

Due to the nature of openness of VoIP protocols (SIP and H.323) and the vulnerably that is associated with IP based real-time services such as VoIP permits attacks by malicious users or clients. VoIP evidence are identified by comparing the abnormal and normal voice packets during VoIP communication [10]. [20] proposed a digital forensics evidence procedure for VoIP network forensics. One such digital forensics evidence procedure is Digital Evidence Forensics Standard Operating Procedure (DEFSOP) for VoIP network forensics. VoIP DEFSOP is based on [21] Prevention and Protection are connected to security, while Preservation and Presentation are connected digital forensics. These is called the Four P's i.e 4Ps. [22] DEFSOP is made up of four (4) stages namely Concept Stage, Preparation stage, Operation stage and Report stage. These four stages form are broken down as shown in Figure 4 which shows VoIP-DEFSOP structure with 4P's Model.

The Concept Stageis the first stage of VoIP-DEFSOP, the concept stage deals with a set of procedural rules for forensics by the first responder (an Investigator) to abide by. The first responder should be familiar with the information in forensic guide and perform his duties and responsibilities ascircumstances dictate. This ensures evidences collection is done following procedural rules with warrant and also ensures obtaining digital evidence legally without violating other information found on the compromised devices.

so, it can also be determine by court judgment. The operation stage recognize, identify, seize and secure all digital evidence at the scene. Documents the entire scene and the specific location of the evidence found. Collect, label and preserve the digital evidence and finally package and transport digital evidence in a secure manner. The Report Stage is the final stage of the VoIP-DEFSOP. This is where courts make judgments based on collected and analyzed forensics evidence obtained at the scene of the crime [21, 22]. In other to identify or collect forensic evidence and investigates, VoIP packet need to be collected in real-time and stored for forensics analysis. In the next section, we discuss VoIP network traffic capturing techniques.

mVoIPc FORENSICS ANALYSIS

Digital forensic is a technology to identify, collect, examine, analyze, and still preserve the integrity of the digital evidence such as data, finger prints etc. These crimes are usually in modern high technology. [23]. Cloud computing, which is designed to support and provide large-scale data processing, to support on-demand services. However, to support forensic investigation and examination on the cloud, especially on real time applications such as VoIP, multiple challenges such as the inability of computer systems to make use of information among current forensic investigation tools, technique and models must be overcome[24, 25]. Current VoIP forensics analysis (VoIPEM, VoIP-NFDE and VoIP-DEFSOP) outlines and models depend on network traffic analysis techniques such as Logging, packet marking, forensics intrusion tolerance, forensics Examination, and interaction. VoIP forensics investigator or first responder adopt these network traffic analysis techniques to record, store, examine VoIP packet, and may be reconstruction attack situations.

The distributed nature and the layered network structure of the cloud presents two critically challenge to digital forensics investigators, first, is the large surface area of investigation due to the distributed nature of the cloud and secondly the restrict access of the internal Document Control Number and Internal Control Number (DCN and ICN) cloud network to forensics network traffic analysis techniques. The latter further complicated evidence identification, gathering and analysis on MVoIPc because critically VoIP component such as Registration server, SIP server are placed within the internal network. To overcome these cloud forensics challenge, we propose to develop a hybrid digital forensics investigation framework, which consist of Forensics-as-a-Service from the Cloud Service Providers (CSPs) and a VoIP forensic investigation model called VoIP-Cloud Forensics Evidence Model (VoIP-CFEM). This proposed model enables forensic investigators access too critically analyzes forensics evidence without compromising the internal CSPs network and most specially the privacy of the cloud users or clients.

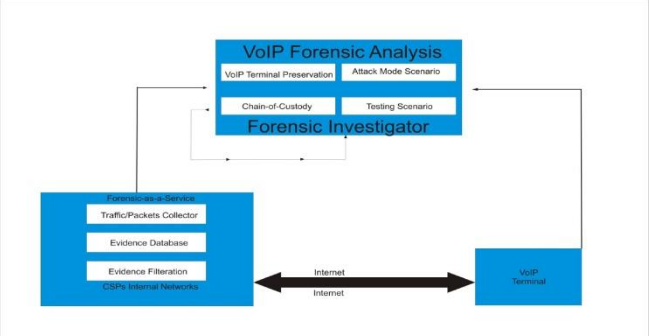

Fig. 5. VoIP Forensic Analysis Model

From the Figure 5 shown, the proposed cloud forensics MVoIPc-IM. The proposed model consists of two components, the Forensics-as-a-Service Evidence Accumulator FEA and Forensics Investigation Procedure (FIP). The proposed model is designed to ensure critically forensics data are collected, stored and filtered without compromising the privacy of a user or client. The proposed model also eliminated the interoperability of current VoIP forensics investigation techniques. We take a critically look at each of the component of the proposed model. First component (FEA) of the proposed model is designed to collect, stores and fitter VoIP data in real-time. It collects VoIP packet from different VoIP components that resides within the CSPs internal network. The FEA consist of three components namely the Traffic/Packet Collector, Evidence Database and Evidence Filtration.

The Traffic/Packet Collector component of the FEA gathers network traffic request and VoIP packet the Real Time Transport Protocol (*which delivers audio and videos over IP network)* and Real Time Control Protocol *(use to monitor transmission and quality of service)* (RTP and RTCP) between user VoIP terminal and VoIP server. Such component includes SIP Authentication and Registration server. Evidence Database, this stores collected VoIP network packet. Evidence Filtration, the stores data is filtered in other to ensure the privacy of other users. The second component of the proposed MVoIPc-IM is the Forensics Investigation Procedure (FIP). The procedure aims to address the challenges of interoperability of current VoIP forensics investigation models by granting access to CSPs data. FIP consist of four (4) sub-components namely Chain-of-Custody, VoIP Terminal Preservation, Attack Mode Scenario and Reporting.

Chain-of-Custody: The chain of custody refers to the documentation or paper trail, showing the seizure, collection, control, transfer, receipt, analysis, storage, and disposition of the digital and electronics evidence. A chain of custody is also validating how any kind of evidence (Digital or Electronics) have been collected, tracked and protected. Chain of custody must answer the following questions. Where is the evidence? How did the analyst get it? When was it collected, who and who handled it? Why the mentioned person did handled it? Where the evidence was ultimately stored? The investigator should ensure that he knows each step the person to whom the evidence was handled over. He must also ensure that such persons has an approved authority to have the evidence in his custody. This ensures that any results we report relate beyond all reasonable doubt to a particular crime in a court of law [26]. In this paper, the author will consider forensics cloud data collected from CSPs has a tool for forensics investigations.

CONCLUSION

Due to increase in the use of VoIP application has advanced the increased research by academia and Telecommunication Companies (TC) or Network Service Providers (NSP). Using the Cloud, VoIP are virtualized on servers to be accessed on-demand. This make VoIP application over the cloud easily installed, configure and rapidly deployed with little management by CSPs. The openness nature of VoIP protocols (SIP and H.323) and the inherit vulnerability associated with IP based real-time services such as VoIP permits such systems susceptibility to attacks by malleolus users. The benefits of using VoIP over cloud, presents forensics challenge to digital forensics investigator. In conducting network forensics investigations in a VoIP environment, the collection of voice packets in real time and the use of automatic mechanisms are fundamental.

This presents three critically challenge forensics investigators. The first is the distributed characteristics of the cloud, secondly the large investigation area covering different location geographically. Thirdly the restrictive nature of the internal cloud network infrastructure and the lack of interoperability of current VoIP forensics (VoIP-NFDE and VoIP-DEFSOP) investigation framework and models. We proposal developing a hybrid digital forensics investigation framework which consist providing Forensics-as-a-Service from the CSPs. This proposed model enables forensic investigators access to critically forensics evidence without compromising the internal CSPs network and most specially the privacy of the cloud users or clients.

REFERENCE

[1] P. Andriotis, G. Oikonomou, and T. Tryfonas, "*Forensic analysis of wireless networking evidence of Android smartphones*," in *Information Forensics and Security (WIFS), 2012 IEEE International Workshop on*. 2012..

[2] R. Bhadauria, "A Survey on Security issues in cloud computing and preprint," arXiv: 1109.5388, 2011.

[3] R. Bhadauria, S. Sanyal, "Survey on Security issues in cloud computing and associated mitigation techniques,".

[4] A. J. Duncan, S. Creese, M. Goldsmith, "Insider Attacks in cloud computing. In: proceeding of the trust," Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on 2012. IEEE

[5] E.B. Fernandez, J.C.P., and M.M. Larrondo-Petrie, "*Security patterns for voice over IP networks,*" Proceedings. of the 2nd IEEE Int. Multiconference on Computing in the Global Information Technology, 2007.

[6] J. C. Fernandez, P.a.E.B., "*VoIP network forensic patterns"*.in Proceedings of the 4th International Multi-Conference onComputing in theGlobalInformationTechnology (ICCGI '09),, August 2009. 180: p. 175.

[7] N. Gupta, and A. Agarwal. "*Context aware Mobile Cloud Computing: Review,*" in *Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on*. 2015.

[8] Y. Guang, , B. Jun, and A.V. Vasilakos, "*Passive IP Traceback: Disclosing the Locations of IP Spoofers From Path Backscatter,"*. Information Forensics and Security, IEEE Transactions on, 2015. 10(3): p. 471-484.

[9] F. GEREA,,"*Implementation of Cloud Computing into VoIP"*. Database Systems Journal, 2012. III, no. 2.

[10] SH Madni, M. S. Latiff, Y. Coulibaly "Recent advancements in resource allocation techniques for cloud computing environment: a systematic review," Cluster Computing. 2017 Sep 1;20(3), pp. 2489-533.

[11] M. M. Ibrahim, M.T. Abdullah, and A. Dehghantanha. "*VoIP evidence model: A new forensic method for investigating VoIP malicious attacks*". in*Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on*. 2012.

[12] I-Long Lin, Y.-S.Y., Bo-Lin Wu, Hsiang-Yu Wang, *VoIP Digital Evidence Forensics Standard Operating Procedure (DEFSOP).* International Conference on Broadband, Wireless Computing, Communication and Applications, IEEE, 2010.

[13] Juan C. Pelaez, E.B.F., *Network Forensics Models for Converged Architectures.* International Journal on Advances in Security, 2010,.vol 3 no 1 & 2.

[14] J, et al. *(Im)proving chain of custody and digital evidence integrity with time stamp*. in*MIPRO, 2010 Proceedings of the 33rd International Convention*. 2010.

[15] SH Madni, Latiff MS, Abdullahi M, Usman MJ. Performance comparison of heuristic algorithms for task scheduling in IaaS cloud computing environment. PloS one. 2017 May 3;12(5):e0176321.

[16] Kotwal, P.A. and A.R. Singh. *Evolution and effects of mobile cloud computing, middleware services on cloud, future prospects: A peek into the mobile cloud operating systems*. in*Computational Intelligence & Computing Research (ICCIC), 2012 IEEE International Conference on*. 2012.

[17] Khan, S., et al., *A Comprehensive Review on Adaptability of Network Forensics Frameworks for Mobile Cloud Computing.* The Scientific World Journal, 2014. 2014: p. 27.

[18] Kuhn, D.R. Walsh, T.J; Fries, S. Special Publication 800-58: Security Considerations for Voice Over IP Systems; NIST: Gaithersburg, MD.USA,2005.

[19] Latiff MS, Abdul-Salaam G, Madni SH. Secure scientific applications scheduling technique for cloud computing environment using global league championship algorithm. PloS one. 2016 Jul 6;11(7):e0158102.

[20] Kumar, R. and S. Rajalakshmi. *Mobile Cloud Computing: Standard Approach to Protecting and Securing of Mobile Cloud Ecosystems*. in*Computer Sciences and Applications (CSA), 2013 International Conference on*. 2013.

[21] Lin, I.L., et al. *VoIP network forensic analysis with digital evidence procedure*. in*Networked Computing and Advanced Information Management (NCM), 2010 Sixth International Conference on*. 2010.

[22] Osanaiye, O., Choo K-K.R., Dlodlo , M. 2016. Distributed Denial of Service (DDOS) resilience in cloud: review and conceptual cloud ddos mitigating frame work

[23] Pelaez, J.C. and E.B. Fernandez. *VoIP Network Forensic Patterns*. in*Computing in the Global Information Technology, 2009. ICCGI '09. Fourth International Multi-Conference on*. 2009.

[24] Pelaez, J.C., *Voip network security and forensic models using patterns*. 2007, Florida Atlantic University. p. 187.

[25] RohasNagpal. Introduction to cyber crime investigation, Asian School of Cyber Laws published in 2012 p.19-23

[26] SitiRahayuSelamat, R.Y., Shaharin Sahib, Nor Hafeizah Hassan, MohdFaizalAbdollah,

ZaheeraZainalAbidin, *Traceability in Digital Forensic Investigation Process.* IEEE conference publication, 2011: p. 101-106

[27] Sally, J., *Major Reasearch Issues in Forensic Computing*.nineth "2007 Internet Space: Information, Laws and Society," TheoriticalReasearch and Practice Coriference,, 2007.

[28] W. Ren, H.J., *Distributed Agent-based Real Time Network Intrusion Forensics System Architecture Design.* Proceedings of the 19th International Conference on Advanced Information Networking and Applications, 2005

[29] Yanik, T., et al. *Evaluating SIP proxy servers based on real performance data*. in*Performance Evaluation of Computer and Telecommunication Systems, 2008. SPECTS 2008. International Symposium on*. 2008.