Cloud Collaboration for Forensically Ready Cyber Space

Bruno Opara, Princewill Akpojotor, Oluwatope Ayodeji, Adesola Aderoumu
Department of Computer Science & Engineering, Obafemi Awolowo University, Ile-Ife, Nigeria

ABSTRACT — The major challenge of forensic investigation of networked systems is the lack or incompleteness of relevant evidence collected for the specific crime being investigated. In cloud networks, acquisition of irrelevant data together with evidential data is also a challenge imposed due to multitenacy in cloud architectures. When employed for a single-cloud or multi-cloud environment, these techniques lead to incompleteness of digital evidence and most times raises integrity concerns. Thus, cloud forensic is faced with the challenge of widely spread evidentiary data in the cloud and existing approaches do not harness evidence sufficiently in a manner suitable for complete of acquisition of evidence. This is because there are missing forensic considerations and capabilities in current cloud computing deployments that can be leveraged upon towards achieving a forensic ready cloud environment. In order to offset some of these challenges, there is need for the development of a novel cloud forensic framework with a collaborative forensic capability model, which acquires evidentiary data proactively and reactively within a multi-cloud environment. This work leverages the multi-cloud's robustness to acquire and examine exhaustive digital evidence in the cloud for legal prosecution of computer aided crimes.

KEYWORDS — Forensic Science, Digital Forensics, Digital Artefacts, Cloud Computing, Cloud Forensics, Cloud Collaboration, Evidence Corroboration.

1. INTRODUCTION

The more pervasive information technology becomes the more the rise in cyber related crime profile. With the trend in heterogeneity and ubiquity of information technology and mobile devices, new cybercrime patterns and techniques geared towards zero crime evidence have continued to emerge. In other words, as new technologies continue to emerge, they come with new challenges that require different approach to solving them and cloud computing is no exception. This is the reason Forensic Science is becoming an integral part of information technology. In this modern age, it is hard to imagine a crime that does not have a digital dimension. Criminals, violent and white-collar alike, are using technology to facilitate their offenses and avoid apprehension, creating new challenges for attorneys, judges, law enforcement agents, forensic examiners, and corporate security professionals (Casey, 2011). The emerging technologies and pervasiveness of cybercrime continues to constitute a big challenge to forensic investigation. Computer related and computer-aided crimes now abound, especially in these days of ubiquitous cloud computing with high-level of sophistry that leaves no trace of evidence behind. Invariably, the emergence of cloud computing came with great opportunities but are now being exploited for cybercrimes and computer-aided crimes.

2. DIGITAL ARTIFACTS IN THE CLOUD

NIST (2011) describes digital forensics as an applied science for "the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data". Cloud forensics can then be defined as applying all the processes of digital forensics in the cloud environment and does include investigating file systems, process, cash, and registry history (Zawoad et al., 2013). Essentially, it is a branch of digital forensics that deals with the processes and procedures for the acquisition of digital artifacts in the cloud for the purpose of preservation and presentation in court of law as admissible evidence. Ruan et al. (2012) defined cloud forensics as a subset of network forensics given the fact that cloud computing is based on extensive network access, and as network forensics handles forensic investigation in private and public network. Digital forensics is a multidisciplinary domain faced with the challenge of widely spread evidentiary data in the cloud which existing approaches do not harness for evidence corroboration. Thus, making the phenomenon of incompleteness of evidence a major problem in digital forensics amongst others. Whereas, digital evidentiary acquisition process must be a rigorous exercise that ensures that no relevant evidence is left out in order to stand the test of legal scrutiny. The lack of completeness of evidence has stalled many crime-related prosecutions and sometimes even exploited in the law courts. There are agitating questions as to who owns the data and which country's jurisdiction and IT law would apply to clouds seating in several geographies. Privacy is another issue. Incident response and computer forensics in cloud environment require fundamentally different tools, techniques and training. Generally, trust of acquired evidentary data is very important in digital forensic. In traditional forensic, there has to be trust in the operating system and hardware to read the disk of a culprits' standalone computer. If the suspect computer was hosted in the cloud, new layers of trust should also be considered. Dykstra and Sherman (2013) stressed the need to understand trust in the cloud environment before delving into the issue of evaluating the tools used for acquisition. This consideration is informed by the fact that in the law court the judge or jury must ultimately decide if they believe and trust the evi-

dence presented to them. The trust factor is all about whether the result is accurate, reliable and complete.

3. NEED FOR CLOUD COLLABORATION

The concept of cloud collaboration is gaining a lot of attention in recent times and can potentially redefine the evidentiary data acquisition from the cloud. The trend is such that the research community is beginning to develop architectures, technologies, and standards to support collaboration among multiple cloud systems. Collaboration among multiple cloud-based services, like cloud mashups, opens up opportunities for Cloud Service Providers (CSPs) to offer more-sophisticated services that will benefit the next generation of clients (Signhal et al.,2013). Signhal et al. (2013) maintain that realizing multi-cloud collaboration's full potential will require implicit, transparent, universal, and on-the-fly interaction involving different services spread across multiple clouds that lack pre-established agreements and proprietary collaboration tools. Invariably, mechanisms for collaboration across multiple clouds must undergo a rigorous, in-depth security analysis to identify new threats and concerns resulting from collaboration. They must have the support of innovative, systematic, and usable mechanisms that provide effective security for data and applications. Such security mechanisms are essential for gaining the trust of the general public and organizations in adopting this new paradigm. Research proposals still remain constraining due to their provider-centric approaches that require CSPs to adopt and implement the changes that facilitate collaboration—changes such as standardized interfaces, protocols, formats, and other specifications, as well as new architectural and infrastructure components. It is expected that the march towards collaboration will continue to be on the upward trend. However, it must be acknowledged that since forensics is increasingly team effort (Garfinkel, 2010), forensic tools need to support collaboration as a first class function. Additionally new collaboration modes need to be discovered and implemented so that users can collaborate in real time, asynchronously, remotely and even on disconnected networks.

4. RELATED WORK

Singhal et al. (2013) proposed a proxy-based multi-cloud computing framework allows dynamic, on-the-fly collaborations and resource sharing among cloud-based services, addressing trust, policy, and privacy issues without pre-established collaboration agreements or standardized interfaces. They proposed framework for generic cloud collaboration allows clients and cloud applications to simultaneously use services from and route data among multiple clouds. This framework supports universal and dynamic collaboration in a multi-cloud system. It lets clients simultaneously use services from multiple clouds without prior business agreements among cloud providers, and without adopting common standards and specifications. Proxies can facilitate collaboration without requiring prior agreements between the cloud service providers. Researchers and industry specialists have highlighted several security issues in cloud computing, including isolation management, data exposure and confidentiality, virtual OS security, trust and compliance, and mission assurance. Specific security issues emerge during dynamic sharing and collaboration across multiple clouds. In particular, issues pertaining to trust, policy, and privacy are a concern in multi-cloud computing environments (Singhal et al., 2013). Shields et al. (2011) proposed a proof-of-concept for PROOFS, a continuous forensic evidence collection system that applies information retrieval techniques to file system forensics. PROOFS creates and stores signatures for files that are deleted, edited, or copied within such a network. The heart of each signature is one or more fingerprints, generated based on statistical properties of file contents, maintaining semantics while requiring as little as 1.06% of the storage space of the original file. In their work, Chen et al. (2010) proposed a practical Collaborative Network Security Management System with well deployed collaborative UTM (Unified Threat Management) and traffic probers. The distributed security overlay network with a centralized Security Center leverages a Peer-to-Peer communication protocol used in UTM's collaborative module and virtually interconnect them to exchange network events and security rules. Also security functions for UTM share security rules.

5. ACHIEVING EVIDENCE CORROBORATION WITH CLOUD COLLABORATION

As the legal requirements for admissibility of crime evidence continues to widen in scope and complexity the task of evidence corroboration becomes more challenging. This situation demands a new approach which makes evidence collaboration a necessity and realizable in a multi-cloud environment. Evidence corroboration breeds evidence corroboration. When different clouds collaborate to share and use evidentiary data the probability of evidence corroboration will be significant and compared to non-collaborative approach. Collaboration will ensure that all relevant sources of evidence for a cybercrime are searched exhaustively before concluding on the case. There have been instances in which cases were thrown out for want of enough evidence while some already concluded cases were rescinded as a result of emergence of fresh evidence. This informs the motivation for this work which is to ensure that whenever cyber-related or aided crime incident is reported, there should be enough collaborative evidence to corroborate the occurrence of the crime that will satisfy legal requirements of evidence admissibility. Cloud forensics is at its infancy and faced with challenges in technical, organizational, and legal dimensions (Ruan and Cathy, 2013) as well as promising opportunities (Ruan et al., 2011). There are missing forensic considerations and capabilities in current cloud computing deployments that can be leveraged upon towards achieving cloud forensic readiness. On the other hand, the existing digital forensic tools for investigating cyber-related crimes are reactive rather than proactive. In other words, they react to crime incidents that have already occurred. This is not helping forensic investigation, especially in today's current reality of information explosion and user-empowering mobile devices that can potentially undermine digital forensics efforts. The emerging information technologies like cloud computing can bring a paradigm shift to digital forensics. There is useful and helpful information about everyone in the cloud which can be used as potential evidence

in the future. At one time or the other, people have given out useful information about themselves or their activities that can help track their lifestyle. There are relevant information about people and their activities, especially crime-related activities (like child pornography) in the cloud that can be used as forensic evidence when the need arises. However, all these information no longer resides locally or in one place but are stored in geographically dispersed locations that transcend multi-jurisdictions. There is a shift towards multi-cloud infrastructure due to high availability of service. However, with this shift multi-cloud culture also means that cybercrime data will be migrating from cloud to cloud. The aggregation and usability of these evidentiary data from various sources for cyber-related crimes will require that the major actors, cloud providers, cloud consumers, cloud brokers, forensic investigators and law enforcement agents to work together cooperatively and collaboratively, especially in a multi-cloud environment. From the foregoing, there exists a procedural problem that has to do with digital forensic phases not keeping pace with current technology. Apparently, the existing digital forensics frameworks and ontologies are not able to take advantage of the possibilities of current technology for evidence robustness. It is no doubt that these traditional forensic frameworks predated cloud computing. However, with the emergence of cloud computing technology this traditional procedural problem can be solved by introducing collaboration as a vital phase in digital forensic framework and modeling it. The footprints of cybercrimes and cyber aided crime can no longer be tracked only in a single cloud but in a multi-cloud environment. There is also the problem of incompleteness of evidence necessary to forensically corroborate and establish occurrence of crime incidents beyond reasonable doubt. This problem has on many occasions resulted in inconclusive judicial proceeding for lack of sufficient evidence as well as retrying of cybercrime cases when more evidence is discovered. The highlighted problems will require a collaborative approach both proactively and reactively in order to achieve a more robust and exhaustive evidence corroboration.

6. PROPOSED COLLABORATIVE CLOUD FORENSIC FRAMEWORK

The proposed collaborative forensic framework for the Cloud computing environment is designed based on the two most widely accepted forensic frameworks for digital forensic-(Mckemmish, 1999 and Kent et al., 2006). These existing frameworks are designed for the traditional digital forensics and therefore lack the capability of handling the recent complexity and the challenges of cloud computing. As an example, these framworks are not robust enough for accessing forensic data in the cloud computing environment, to determine data linkability and accountability in cases where illegal activities are performed. Also, little guidance exists on how to acquire and conduct forensics in a cloud environment, since existing best practice guidelines still apply to digital forensics in the cloud computing environment (NIST, 2011). This may not be a suitable approach to digital forensic in the cloud environment. Thus, there is clearly an urgent need for a forensic framework specific to the cloud environment that should adapt and augment technical and procedural forensic responses, while retaining the legal requirments of evidence presentation to the courts.The proposed framework also combines the identification and preservation of evidence sources as adopted from Martini and Choo (2012) who proposed an integrated digital forensic framework to conduct digital forensic investigation specific to the cloud computing environment, based on iteration between the first phase (identification and preservation) and the third phase (examination and analysis). This approach ensures the preservation of cloud computing data as soon as an incidence is reported. Since the goal of the design was on prompt identification and preservation of cloud computing data, not much emphasis was placed on the complexity and increasingly time consuming process faced with acquisition of evidentary data as experienced in the cloud environment. The proposed collaborative cloud computing forensic framework depicted in Figure 1.1 introduces a collaborative phase with iteration between the collaborative phase and acquisition/collection phase. Introduction of a collaborative phase will foster the speed of evidentary data collection distributed across multiple platforms. Also, adopting iteration between the collaborative and acquisition phase is a necessary step towards a forensic ready cloud computing environment for updated acquisition as well as preservation of captured data. The proposed framework consists of six phases with the inclusion of a new collaborative phase suitable for a multi-cloud environment. These phases include Identification, Preservation, Collection, Collaboration, Examination and Analysis and Presentation.

i. Identification Phase

This phase defines the requirement for evidence management, determining its presence and its location as well as its type and format. The phase focuses on identifying the source of evidence both proactively and after an incidence report (reactively). At this stage, sources of evidence identified within the multi-cloud will include cloud services/providers and hardware storage facilities with cloud providers. Identification of cloud services used on the seized hardware may be easily identified from artefacts such as login credentials and cache data. These artefacts are also used as pointer to identify and/or locate alternate sources of evidence.

ii. Preservation Phase

This phase is concerned with ensuring that potential and acquired evidential data remain unchanged. The preservation phase requires the cooperation of the Cloud Service Provider to

- *Bruno Opara is currently pursuing doctorate degree program in computer science and engineering in Obafemi Awolowo University,Ile-Ife, Nigeria*
- *Princewill Akpojotor is a graduate assistant in computer science and engineering department in Obafemi Awolowo University, Ile-Ife, Nigeria*
- *Ayodeji Oluwatope is a doctor in computer science and engineering department in Obafemi Awolowo University, Ile-Ife, Nigeria*
- *Adesola Aderounmu is a professor in computer science and engineering in Obafemi Awolowo University, Ile-Ife, Nigeria*

place a hold on identified accounts and prevent any further changes to data after an incidence response. Two forms of preservation is considered in this work. Firstly, the preservation of data of interest after the identification of suspected cloud service or while court proceedings are being undertaken. Secondly, a proactive approach of storing and preserving possible or potential evidence with the cloud provider.

iii. Collection Phase

This phase is concerned with the capture and acquisition of dataset that are possible, potential and identified evidential data. Since the scope of this work is limited to IaaS (Infrastructure-as-a-Service) deployment model, the two major focused form of retrieval are virtual hard disk and memory provided to the user. Acquiring some of this data will require live forensics, which is an approach employed for proactive acquisition of evidential data. Due to the complexity of the multi-cloud environment (distribution of data centres, shared storage resources), evidential data could be mixed with data from other cloud consumers during retrieval. Thus, there ia a need for the collection phase to be made a single stand-alone step for effective filtering and performance. In this stage, iteration is introduced with the next phase for proactive and reactive data acquisition. Proactive data acquisition employs live forensics means and techniques of obtaining artefacts of evidential value (e.g disk image snapshot and current memory) while the machine is running.This proactive acquisition involves capturing virtual disks and current memory from the target cloud service via API, while it is still running rather than capturing an image of the entire server which holds the data. These data are used as potential evidential sources in the cloud computing investigation. Reactive data acquisition is a response to an incident report and collaborates with the next phase for effective acquisition of evidential data (e.g metadata) from the suspected cloud customer/cloud service. It then proceeds to retrieve relevant evidential data from other clouds with related information based on data acquired from suspected cloud customer/cloud service. For the acquisition of possible and evidential data from the cloud proactively and reactively appropriate existing standard tools are used. Also, this phase requires the cooperation of the Cloud Service Providers and its Application Programming Interface (API) to provide relevant data. Data retrieved in this phase are copied and hashed for integrity purpose.

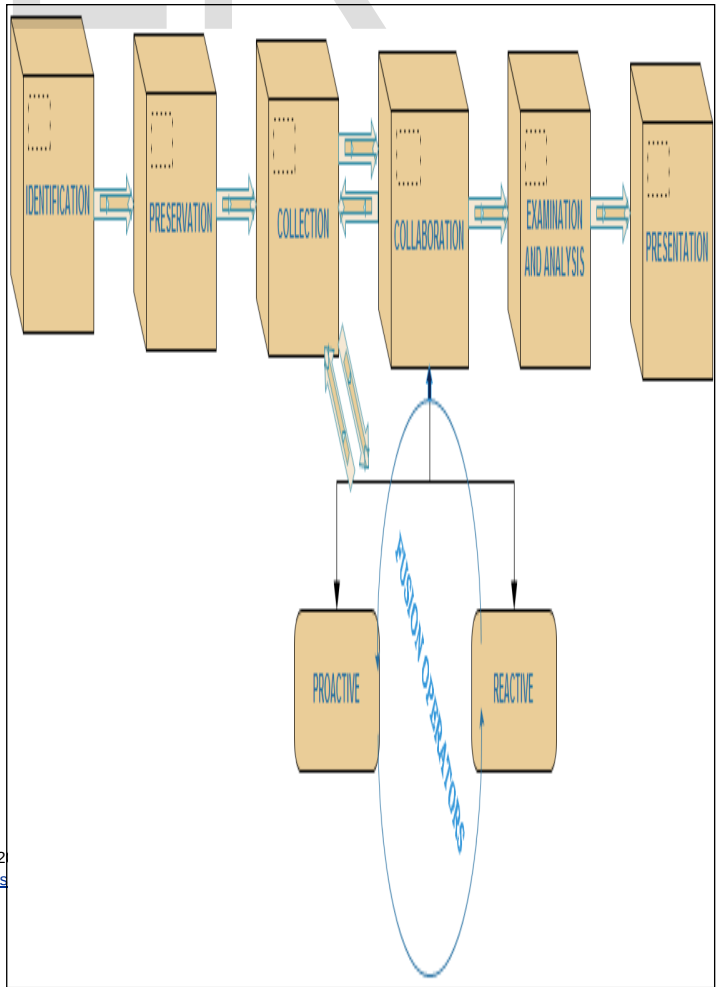
iv. Collaboration Phase

The introduction of this stage is to ease the complexity of data acquisition within the multi-cloud environment. Since cloud customer data are scattered across different cloud storage and share same cloud resources, evidence gathering becomes a complex task. This phase cooperates and works simultaneously with the collection phase for data retrieval both proactively and reactively. It uses fusion operators to combine the proactive data acquired at the collection phase with the reactive evidential data retrieved after an incident report. The result of this is a pattern match and extraction of all relevant evidential data that should be used by a Central Forensic Management System (CFMS) to coordinate further search and retrieval of related evidential data from other cloud sources. At such, iteration is established between the collection phase and the collaboration phase to perform live forensics (proactive acquisition) and reactive acquisition in response to directives from the CFMS.

v. Examination and Analysis Phase

This stage is concerned with extraction and derivation of data of interest and transforming this data into suitable format. The examination and analysis phase are put together because not all evidential data requires examination. If the evidential data captured from the cloud is in a suitable format then forensic investigator need only to conduct analysis, but if otherwise, then examination is required to reconstruct the suspect activities from the collected abstract data. However, examination is an important step for data collected from a cloud computing environment as the evidential data is likely to be captured in an unsuitable format that would not permit direct analysis. Since the focus is on IaaS (Infastructure-as-a-Service), a major dataset to be analysed by the forensic investigator is a virtual image of a running machine which holds all data uploaded by the suspect. This data most times does not come in a suitable format that requires direct analysis, hence there is need to examine the data using suitable tools to deal with an unreadable format.

vi. Presentation Phase The final phase is concerned with presenting evidence provided by forensic expert after analysis in a suitable manner to a law court. Since it involves legal presentation, this work retains the general digital forensic presentation phase without any changes. This phase remains similar to the



framework of McKemmish and NIST.

Fig: 1.1 Conceptual Framework of the Proposed Model

7. ARCHITECTURAL OVERVIEW OF DESIGN

The proposed architectural design for the collaborative cloud forensic model allows each of the cloud service providers to host a forensic data management module for proactive and reactive forensic data management. These data management modules communicate with a Central Forensic Management System deployed as an Autonomous Cloud, whose responsibility is to make collaboration between Cloud Service Providers possible. This architecture supports universal and dynamic collaboration in a multicloud system for forensic purposes. A collaborative forensic multi-cloud architecture is depicted in Figure 1.2. A multicloud collaborative forensic system that employs data management modules communicating with a central forensic management system hosted as a service in an Autonomous Cloud is proposed. This architecture consists of three major components: Data Management module, Central Forensic Management module (CFM) and Multiple Cloud Computing System. Each Data Management module is cloud-hosted for a specific cloud. That is, every Cloud Service Provider within the multi-cloud network hosts a Data Management module within its cloud infrastructure and manage this module within its administrative domain. Each of these modules deployed within a cloud are cloud specific and can handle requests for forensic response (incidence response) in that cloud and communicates with the Central Forensic Management System for subsequence response. The Data Management module consists of two submodules, the Proactive Data Management (PDM) and the Reactive Data Management (RDM) which perform forensic data acquisition proactively and reactively respectively. In turn, the Data Management module combines their data using some fusion operators to extract core and related forensic data in the order of relevance, which is to be used as parameters in communicating with the Central Forensic Management module.

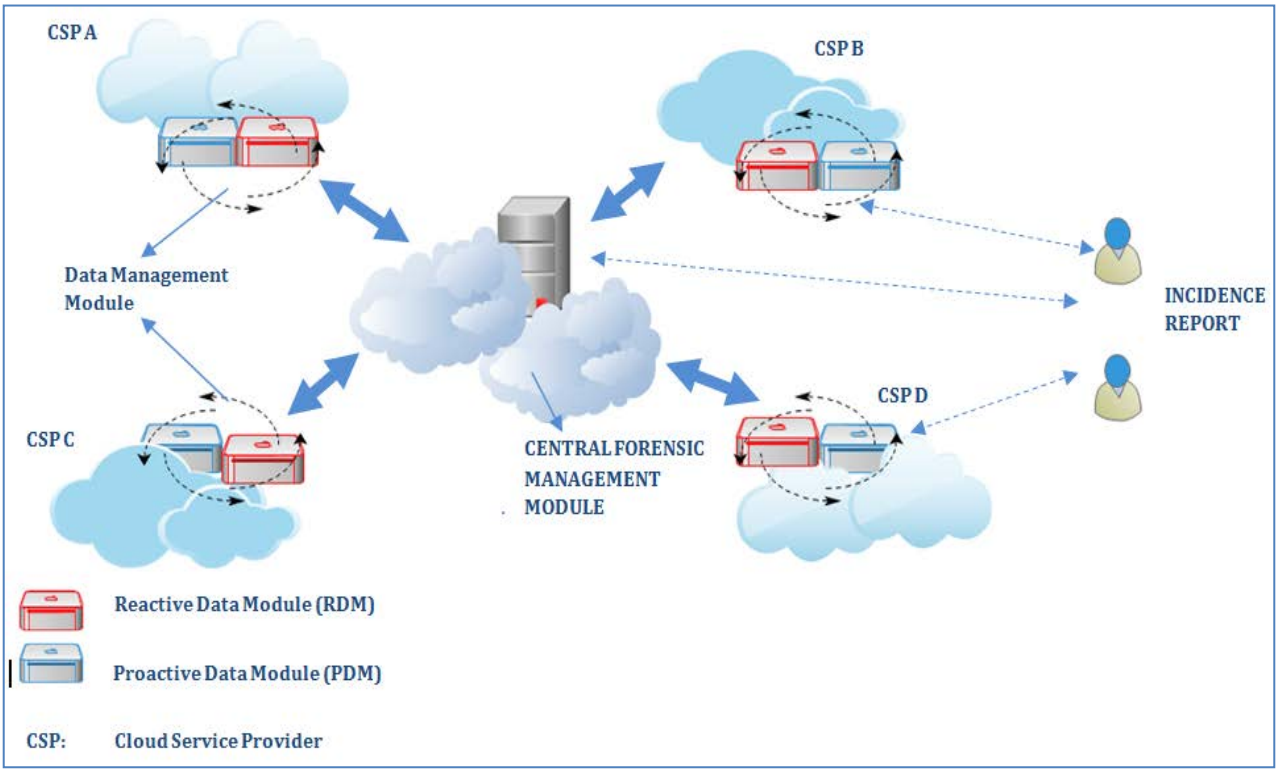


Fig. 1.2: Architectural Overview for Collaborative Forensics

The Central Forensic Management module is service-hosted in an autonomous Cloud. That is, the management module is hosted as a Forensic-as-a-Service (FaaS) in a Cloud and offers collaborative services as well as data management for forensic agents and Cloud Service Providers. The Central Forensic Management System receives request directly from forensic agents and a group of Cloud Service Providers within the multi-cloud and employs a peer-to-peer means of communication and interaction for collaboration with the rest of the Cloud network. Thus, a forensic agent can send a request to Cloud C, Cloud D or the Central Forensic Management System, which dynamically discovers the need to interact with other Clouds within the network. Developing this architecture serves as the first step in building a module-based, collaborative forensic multicloud computing environment.

7.1 PROACTIVE DATA MANAGEMENT MODULE

The Proactive Data Management (PDM) sub-module integrated within the management server of the Cloud Service Provider stores the dataset acquired prior to an incident report. This part of the architecture enhances the overall system by performing live forensics. That is, it employs means and techniques of obtaining artefacts of evidential value from a machine that is running at a particular point in time. This is a routine process and involves exporting data such as virtual disks and current memory via an API from the entire server that holds data. Proactive acquisition of data provides access to data stored on a cloud service in a timely manner and it is a step towards enhancing forensic readiness. Figure 1.3 depicts the structure of the PDM. The PDM enables the system to inspect cloud hosted virtual machines and extracts virtual machine snapshots. This acquisition is a collection of various virtual disk images, memory and log files in a data server as potential source of evidential data in the future. This data management module consists of a database for storing the relevant dataset, data mining system and fusion operation module. The database comprises monitored data, services artefacts and logs obtained during the proactive acquisition of suspicious crime data. The datasets coming from the cloud environment are collected from multiple tenants and stored in three forensic database sub-systems. The system activity and collection of data runs periodically to obtain up-to-date versions of information. The acquisition of dataset from the cloud architecture is done using an existing forensic acquisition tool connected to the cloud management software via the dedicated Open Virtualization Format (OVF) communication channels. The OVF is a standard language suitable for both the design of distributed applications for the Cloud. OVF exploits the XML standard to establish the configuration and the installation parameters. Also, it is capable of creating and distributing software applications to be executed on different VMs, independently from hypervisors and CPU architectures.

7.2 REACTIVE DATA MANAGEMENT MODULE

The Reactive Data Management (RDM) sub-module which is integrated within the management server of the Cloud Service Provider acquires and stores core crime data after an incident report. The incident report could be requested from a particular Cloud Service Provider or from the Central Forensic Management System, which in turn relates with other Cloud Service Providers to retrieve core crime related data. Based on details of

the request from crime incidence, the RDM obtains specific data such as log file and metadata from suspect VM and uses these details to interact with the proactive module so as to extract relevant data from a mass of data acquired proactively. After this combination, the extracted data are then uploaded to the Central Forensic Data Management module (CFDM) for subsequent processes. Such information obtained are used to tie a suspect to several files within the multicloud management system. Figure 1.4 depicts the Reactive Data Management subsystem. As depicted, the RDM comprises forensic database module and data management module interacting with the suspect virtual machine. The forensic database module holds evidential data after its retrieval from the client's virtual machine and the data management module carries out some specific tasks. The reactive core module comprises four subcomponents: Data Copy, Image Hashing, Data Mining and the Fusion module. The Data Copy sub-component holds a copy of all evidential data prior to encryption at the Central Forensic Management System and integrity hashing. Keeping copies like this helps the system to preserve the original copies when forensic activities are performed. The Image Hashing/Integrity checking is another sub-component necessary for easy search of exact core crime data within the multi-cloud network. Also, it is useful in securing and checking the originality of files. The Data Mining sub-component is responsible for hidden knowledge extraction functions in order to generte the case related digital evidence. Also, the reconstruction of the events timeline takes place in this sub-component. The Fusion Operation subcomponent is used to combine evidence acquired reactively with the proactive module so as to extract all relevant data from the proactive module.

7.3 CENTRAL FORENSIC MANAGEMENT MODULE

The Central Forensic Management module comprises three subcomponents: the Encryption, Data Storage and Fusion module. It is responsible for coordinating the interaction of various clouds within the multi-cloud network. It has embedded algorithms within it for coordinating the interaction of various clouds in other to perform efficient acquisition of evidentiary data. When a request is placed on the Central Forensic Management System, it uses the given parameters to perform search in all the various clouds available in the network. Prior to an incident report, potential evidential data are acquired and stored in the data management module integrated in each Cloud Service Provider's architecture. However, when a request is made after or during an incidence, the Central Forensic Management System uses its management module to prompt the targeted cloud to acquire and store data from suspect Virtual Machine in its reactive data management module. After extraction of core and related digital evidence at the Fusion Module, the Central Forensic Management System stores this extract in it Data Storage module and uses this data for collaboration with other Cloud Service Provider's proactive management module for efficient and robust acquisition. Figure 1.5 depicts the interaction of the Central Forensic Management module with other clouds within the network. The Central Forensic Management module communicates with other cloud via peer-to-peer network using proxies. Each proxy in the peer-to-peer network is an independent entity that manages itself within its cloud. However, within the architecture of various clouds the subcomponents communicate using Open Virtualization Format (OVF) communication channels. The OVF is a standard language suitable for design of distributed applications for the Cloud. The OVF is created and distributed as software application to be executed on different Virtual Machine, independent of hypervisors and CPU's architecture. The OVF is responsible for data transmission from their respective cloud to the correct Forensic Data Base component for the collection activity.

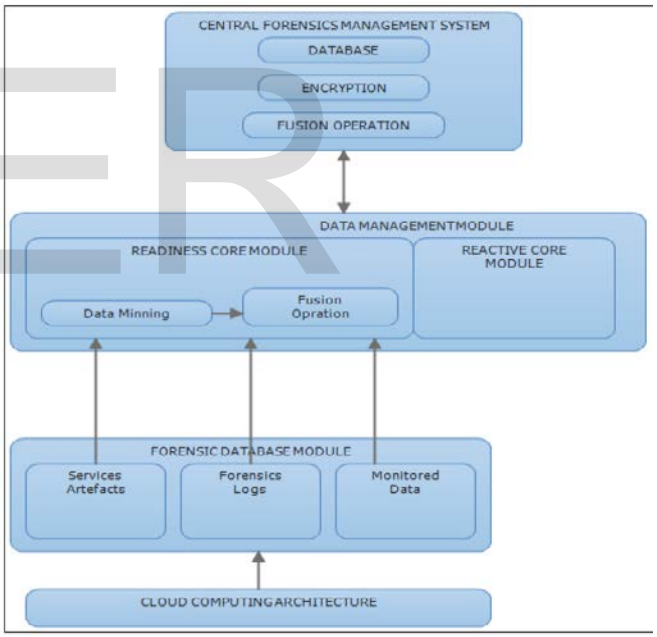


Fig. 1.3: Proactive Data Management Module

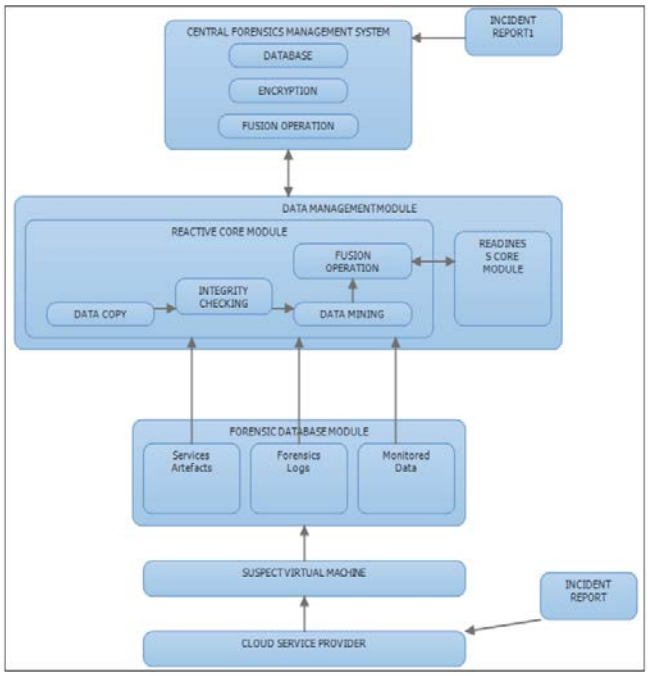


Fig. 1.4: Reactive Data Management Module

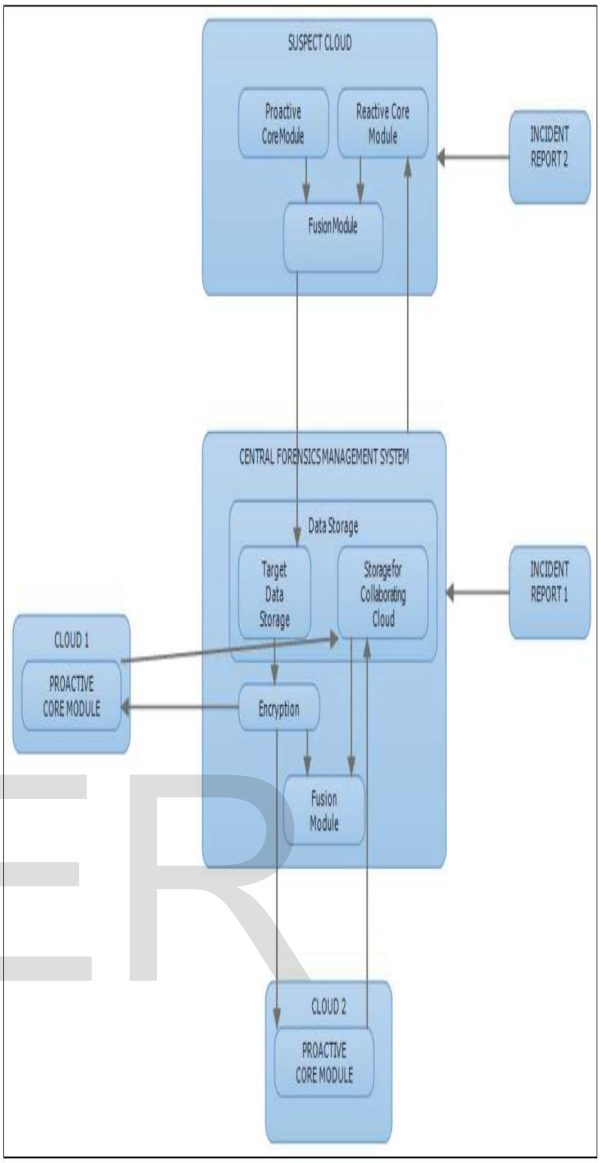


Fig. 1.5: Central Forensic Management Module

8. FUTURE WORK

The motivation for further work is high given the fact that the work is an interesting area of research which is not only novel but connects with the present reality of today. Still riding on the principle that "every crime leaves a trace of evidence", it goes without saying that every cybercrime leaves a trace of evidence or footprints somewhere in the cyberspace. In other words, the cyberspace contains a lot of evidentiary information that can reveal people's lifestyle and predispositions overtime and only waiting to be corroborated when a crime incident occurs. By implication, there is more than enough evidentiary data available in the cyberspace on every cyber –aided or assisted criminal activity. It is possible to build forensic intelligence from the volume of data in the cyberspace (mobile, database, network, computer and cloud) through collaboration which when harnessed will pave the way towards a forensically ready cyberspace.

REFERENCES

[1] E. Casey, "Foundations of Digital Forensics. Digital Evidence and Computer Crime", Third Edition, Elsevier Inc. ISBN 978-0-12-374268-1, pp.3-32, 2011.

[2] Z.Chen, F. Han, J.Cao, X. Jiang and S. Chen, "Cloud Computing-Based Forensic Analysis for Collaborative Network Security Management System". Technical Report, Tsinghua Science and Technology, Vol.18(1):pp.40-50,2013.

[3] J.Dykstra and A.T. Sherman, "Design and Implementation of FROST: Digital Forensic tools for the OpenStack Cloud Computing", The International Journal of Digital Forensics & Incident Response, Vol. (10):pp.587-595, 2013.

[4] J. Dykstra and A.T. Sherman, "Acquiring Forensic Evidence from Infrastructure-as-a-Service Cloud Computing: Exploring and evaluating tools, trust, and techniques". Digital Investigation. Elsevier Journal, Vol. 9, pp. 90-98, 2012.

[5] S.L. Garfinkel, "Digital forensics research: The next 10 years". Elsevier Journal on Digital Investigation, Vol. 7:pp.64-73, 2010.

6] K. Kent, S. Chevalier, T. Grance and H. Dang. "Guide to Integrating Forensic Techniques into Incident Response". Recommendations of the National Institute of Standards and Technology (NIST), 2006.

[7] M. Kohn, J.H.P. Ellof and M. Olivier. "UML Modeling of Digital Forensic Process Models (DFPMs)". Technical Report, Information and Computer Security Architectures (ICSA) Research Group, 2007.

[8] B. Martini and R.K.K. Choo (2012). "An Integrated Conceptual Digital Forensic Framework for Cloud Computing". Elsevier Journal on Digital Investigation, Vol. 9:pp. 71-80, 2012.

[9] R. McKemmish. "What is Forensic Computing? Trends and Issues in Crime and Criminal Justice". Technical Report. Australian Institute of Criminology, No.118, 1999.

[10] NIST. "The NIST Definition of Cloud Computing". Special Publication 800-145. Recommendations of the National Institute of Standards and Technology, 2011.

[11] K. Ruan, J.Cathy, T. Kechadin and M. Crosbie (2012). "Cloud forensics: An overview". Technical Report, Centre for Cybercrime Investigation, University College Dublin, Ireland, 2012.

[12] C. Shields, O. Frieder and M. Maloof. A System for The Proactive, Continuous, And Efficient Collection Of Digital Forensic Evidence. Digital Investigation. Elsevier Journal, Vol. 8:pp. 3-13, 2011.

[13] M. Singhal, S. Chandrasekhar, T. Ge, R. Sandhu and R. Krishnan, G.J.Ahn and E. Bertino. "Collaboration in Multicloud Computing Environments: Framework and Security Issues". IEEE Transactions on Cloud Computing, Vol. 46(2):pp. 76-80, 2013.

[14] S. Zawoad and R. Hasan. "Digital Forensics in the Cloud. Crosstalk". Technical Report, University of Alabama, Birmingham, 2013.