Digital Forensics Evidence Acquisition and Chain of Custody in Cloud Computing

Mahmoud M. Nasreldin[1], Magdy El-Hennawy[2], Heba K. Aslan[3], and Adel El-Hennawy[1]

[1] Ain Shams University
Cairo, Egypt

[2] Shorouk Academy
Cairo, Egypt

[3] Electronics Research Institute
Cairo, Egypt

Abstract

The new cloud computing concept delivers an adaptable service to many users. This is due to the fact that cloud computing offers an economic solution based on pay-per use idea. At the same time, digital forensics is a relatively new discipline born out due to the growing use of computing and digital solution. Digital forensics in cloud computing brings new technical and legal challenges (e.g. the remote nature of the evidence, trust required in the integrity and authenticity, and lack of physical access.) Digital forensics difficulties in cloud computing comprise acquisition of remote data, chain of custody, distributed and elastic data, big data volumes, and ownership. In the literature, there are many schemes that deal with these issues. In 2013, Hou *et al.* proposed a scheme to verify data authenticity and integrity in server-aided confidential forensic investigation. The authenticity and integrity are two essential requirements for the evidence admitted in court. The aim of this paper is twofold. First, to introduce a new concept for digital artifacts acquisition in cloud computing as a consolidation between digital forensic and cloud computing. This concept guarantees safe investigation to trusted digital evidence. Secondly, to analyze Hou et al.'s scheme with respect to its claimed integrity and authenticity properties. Our analysis shows that Hou et al.'s scheme does not satisfy the claimed integrity and authenticity in server-aided confidential forensics investigation. To achieve the authenticity, confidentiality and integrity of evidence in cloud, we illustrate how encryption and digital signature algorithms could be used within different designs to ensure confidentiality and chain of custody for the digital forensics process in the cloud.

Keywords: *Cloud Computing, Digital Forensics, Digital Evidence Acquisition, Digital Investigation, Trusted Digital Evidence, Chain of Custody, Encryption, Digital Signature.*

1. Introduction

Cloud computing is expected to shape the forthcoming practices in Information and Communication Technology (ICT). It is likely that cloud computing will change the approaches in which establishments comprehend their Information Technology (IT) need. Business-wise, cloud computing allows establishments to efficiently subcontract IT needs and reduce the operation cost (e.g. equipment, support, maintenance, manpower.) In cloud computing, establishments transfer their data and processing to a cloud to achieve high availability and access speed. Cloud security is the main anxiety of clienteles in the cloud. So, many establishments resist migration of their IT needs to the cloud.

On the other, hand, digital forensics has developed as a discipline to support law enforcement in dealing with the use of digital device in illegal acts. In the Internet of Things era, gadgets feature in many of the everyday crimes. In cybercrimes, forensic inspection of digital evidence can disclose a fortune of clues. Given that an incident took place, it is vital to the law and order to be able to enquire into the evidence in order to assure that the evidence is admissible in court. This implies how to discover, identify, trace, and handle the cybercrime evidence. It is essential to reconstruct precisely what has been done, otherwise critical evidence might be questioned by court. The digital forensic investigator must follow firm digital forensic methodologies in order to conduct a digital forensic inspection. The digital forensic process comprises a number of steps (i.e. acquisition, examination, analysis, and reporting).

Due to the rapid development in cloud computing, numerous challenges in cybercrime investigations appear. This brings the need for digital forensics professionals to encompass their expertise in the cloud computing and digital forensics domains in order to reduce the risks of cloud security breach. Apart from that, some characteristics of cloud computing such as lack of well-defined physical characteristics, different service models, and different deployment models have created a new

setting for cloud forensics dimensions. Through this paper, we will refer to digital forensic in non-cloud environment as traditional digital forensics, the traditional digital forensics require a specific description to the evidence that will be acquired. This description should include the physical descriptions which are size, media type, the evidence interfaces, and file system format that will be acquired.

Due to the big data and distributed storage, the traditional disk cloning might be unbearable to conduct in gathering evidence in the cloud. On the other hand, shared hosting is common in the cloud. The shared host contains both suspicious material data to the cybercrime and sensitive immaterial information. To protect the privacy of the irrelevant user and enhance the investigation process, the naïve approach is to trust the server administrator in searching, retrieving and handling the relevant data to the investigator. To protect investigation confidentiality and privacy of irrelevant users in forensic investigation (server-aided confidential forensic investigation), Hou et al. [1-2] proposed several solutions. However, the authenticity and integrity of the evidence collected in [1-2] are not considered. The authenticity and integrity are two fundamental requirements for admissibility of evidence in court. In [3], Hou et al. proposed a "encryption-then-blind signature with designated verifier" scheme to prove the authenticity and integrity of the evidence. When data is presented as evidence during a trial, Hou et al. [3] aimed to realize that the administrator (or the third party the administrator trusts) can verify whether the presented evidence is the data that comes from the server and whether the evidence is altered or not. In addition, Hou et al. [3] implemented the proposed system based on commutative encryption and examine its security.

In this paper, we introduce a new concept for digital artifacts acquisition in cloud computing as a consolidation between digital forensic and cloud computing. The aim of the proposed concept is to make sure that the investigation of the trusted digital evidence is safe and show that the cloud is able to support digital forensic investigations. Moreover, we analyze Hou et al.'s scheme [3] with respect to its claimed integrity and authenticity properties. In our analysis, we show that Hou et al.'s scheme [3] does not satisfy the claimed integrity and authenticity in server-aided confidential forensics investigation. In particular, we show that Hou et al.'s scheme [3] is classified as encrypt-then-sign insecure design. We also, present a man-in-the middle attack against Hou et al.'s scheme [3]. Furthermore, we illustrate how encryption and digital signature algorithms could be used within different designs to ensure confidentiality and chain of custody for the digital forensics process in the cloud and prevent man-in-the middle attack.

The remainder of this paper is organized as follows. In the next section, we briefly review the fundamental and technical background of cloud computing. In section 3, we elaborate on digital forensics discipline. The analysis of forensic investigation and implication of digital evidence in cloud computing environment is included in Section 4. Cloud computing evidence acquisition and privacy issues and the consolidation between the digital forensic and the cloud computing are presented in section 5. Our proposed attack against Hou et al.'s scheme [3] and the simple fix to prevent this attack is presented in section 6. Finally, we conclude in Section 7.

2. Cloud Computing

Cloud computing (Internet computing) usually is considered as a collection of clouds on the World Wide Web (WWW). It utilizes the Internet to provide technology enabled services to establishments and users. Using the cloud, users have the ability to access to the WWW anytime/anywhere regardless the maintenance and management requirements in a dynamic and scalable fashion [4-5]. NIST defines cloud computing as a pool of computing resources such as servers, networks, services and applications that provide convenience, flexibility and more performance on demand network access which is consisting of five essential characteristics, three service models and four deployment models. Cloud computing delivers reliable access to distributed resources and it reforms the IT domain due to its rapid accessibility, scalability, less maintenance cost, data and service availability assurance, and services provision infrastructure [6-7]. In cloud computing, concerns regarding overprovisioning services that do not meet their predictions do not exist. Thus, there is no costly waste of resources, or under provisioning for one that turns into wildly popular. This approach reduces the possibility of missing potential customers and revenue. Moreover, establishments with large batch-oriented tasks can get results, as fast as, their programs can scale. Cloud Computing reformed to a new model consists of services that are provided in a similar way to traditional utilities, such as gas, electricity, water, and telephony services. In this model, customers do not bother themselves to know where the services are hosted or how they are provided. Cloud computing considers the infrastructure as a "Cloud" from which businesses and clienteles are capable and capable to access applications from anywhere in the world using on demand techniques.

The potential of cloud computing has been recognized by major industry players such that the top five software companies by sales revenue all have major cloud offerings. There is still no universal definition of cloud computing, however, there is sufficient literature available in the community that portrays the basic principles. The view taken by several authors is that cloud computing is an extension of cluster computing, or more specifically Cloud Computing = Cluster Computing + Software as a Service [9].
What is relatively clear is; cloud computing is based on five key characteristics, three delivery models, and four deployment models.

Cloud computing denotes both the delivered applications as services over the Internet and the hardware and systems software in the data centers. The data center hardware and software form the cloud. The Cloud Computing Service Model is based on three primary tenants: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). In the SaaS , the application is hosted and delivered online through a web browser. In Paas, the cloud provides the software platform for systems. Iaas is a set of virtualized computing resources. All IT roles, such as security, storage, applications, networking, and software work in harmony to provide users with a service based on the client-server model. There are four deployment models for cloud services specific requirements [10]:
- Public Cloud: The cloud infrastructure is available to public or a large industry group. The owner is an establishment that sells cloud services (e.g. Amazon EC2).
- Private Cloud: The cloud infrastructure is operated exclusively for a single establishment and might be managed by the same establishment or a third party (on-premises or off- premises.)
- Community Cloud: The cloud infrastructure is shared by some establishments and supports a specific community with common interest (e.g., security requirements, mission, policy, or compliance considerations) and might be managed by the same establishment or a third party (on-premises or off-premises) (e.g. academic clouds.)
- Hybrid Cloud: The cloud infrastructure is an alignment of two or more clouds (private, community, or public.) It allows data and application portability (e.g., cloud bursting for load-balancing between clouds) (e.g. Amazon VPC).

Cloud computing interact with challenges that might define the degree of utilization (i.e. data and applications interoperability, security, data exchange and transfer, business continuity and service availability, data and applications interoperability, performance unpredictability, storage scalability, bugs in large scale distributed systems, scaling quickly, and software licensing). These five essential characteristics of cloud computing are on-demand self-service, ubiquitous network access, rapid elasticity, Location independent resource pooling and measured service (pay per use). In the next section, we elaborate on digital forensics discipline.

3. Digital Forensics

Digital forensics (computer forensics) is the use of scientific methods for the identification, preservation, extraction and documentation of digital evidence derived from digital sources to enable successful prosecution. The objective of digital forensics is to enhance and acquire legal evidence that is found in digital media. The current NIST definition of digital forensics is the scientific procedures used to recognize and classify, collect, evaluate, and analyze the data while maintaining the level of integrity of the information throughout the forensics process. The purposes of digital forensics are including forensic computing, forensic calculations and computer forensics. Being called into judicial proceedings is one of the digital forensics risks. Thus it must have a correct procedure in conducting the forensic investigation and doing the inspection setup where this procedure or methodology must basically base on the scientific principles [11].

It is essential to have a well-thought-out way of proper handling of evidence in order to minimize errors in investigations. This well-thought-out way is known as the digital forensic process. Moreover, for the trustworthiness of evidence, the digital forensic investigators are typically requested to clarify the process they used in gathering evidence in a court of law. This means that the digital forensic investigator should always know the digital forensic process and the suitable toolsets used in a digital forensic investigation [12-13].

The digital forensic process can be classified into four phases namely acquisition, examination, analysis and reporting. This process is well known in mobile and network forensics fields. Invoke that the authors only focus on the acquisition phase of the digital forensic process in the traditional and cloud computing digital forensics. Thus, the acquisition phase is deliberated in further details. The acquisition phase defines how data will be acquired from different types of digital information sources. Data has to be acquired in a way that maintains its integrity and authenticity. The acquired data has to experience forensic duplication or sector level

duplication. A write blocker should be used in building duplicates. The write blocker guarantees that nothing is written to the original evidence. Software imaging tools can also be used. Imaging could be a physical image (bit-for -bit image) that is created of the entire physical device or a logical image that is created from active directories and files available to the operating system. Hash function is used to verify the integrity of acquired data. Digital hash conducts a mathematical algorithm to provide a fingerprint that authenticates that the data has not been tampered with or altered. This fingerprint is maintained within the case file [14-16].

Several studies that focus on technical issues, challenges and the opportunities have been done, but more research is need to find effective methods to evaluate the uncertainty of the evidence or any forensic findings in the cloud forensics processes. Forensic investigators need to update themselves in multiple disciplines of knowledge in order to investigate the digital evidence in a cloud environment. In particular, they need to acquire high level of knowledge in specific areas such as mobile, hard disk, registry and others that can be considered as legal evidence in court. In order to enhance the digital forensics process in cloud computing, basic framework and architecture are needed. In the next section, we analyze the forensic investigation and implication of digital evidence in cloud computing environment.

4. Cloud Computing Digital Forensics

Cloud computing allows establishments to make use of high scalable infrastructure resources, pay-per-use service, and low-cost on-demand computing. Clouds attract various establishments. However, the security and trustworthiness of cloud infrastructure has become a growing concern. Clouds can be a destination of attacks or a source to launch attacks. Malicious individuals can simply abuse the power of cloud computing and manipulate attacks from nodes/hosts inside the cloud. Most of these attacks are original and exclusive to clouds. Many characteristics of cloud computing make the cloud forensics process complex. In cloud computing, the storage system is not local [17]. Moreover, law enforcement agents cannot seize the suspect's computer/digital device in order to get access to the digital evidence, even with summon to appear. In the cloud, each server/host encompasses files from many users. Therefore, it is not easy to confiscate servers/hosts from a data center without violating the privacy of other users. Furthermore, when identifying data that belongs to a particular suspect, it is difficult to separate it from other users' data. There is no standard way, other than the cloud provider's word, to link given evidence to a particular suspect. So, the credibility of the evidence is also doubtful [18].

In traditional digital forensics, investigators have physical access and full control over the evidence (e.g., process logs, router logs, and hard disks). Unfortunately, in cloud digital forensics case, the control over data diverges in different service models. There are different levels of control of customers' data for the three different service models (i.e. Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)). Cloud users have highest control in IaaS and least control in SaaS. Thus, lack of physical access of the evidence and absence of control over the system make evidence acquisition a challenging task in the cloud environment. In the cloud computing environment, the source of the evidence is ubiquitously and the connection to the source is complicated. Furthermore, the investigators have to hire others (inside/outside the country.) Unlike copying a file from one folder to another folder, the processes of retrieving the evidence in cloud storage is complex. Usually, it costs a lot of time and money in parallel to the investigation time. Investigators have to determine the computational structure, attribution of data, and the integrity of the data. Also, investigators have to keep the stability of evidence and present/visualize it [19-20]. In the next section, we present a new concept for the consolidation between the digital forensic and the cloud computing.

5. Cloud Computing Evidence Acquisition

There are two different ways to include digital forensic investigation in could computing. In the first way, considers the cloud as a tool of the crime. In the second one, the cloud hosts a service as a target of the crime. In this section, we elaborate on the inspection of a targeted system of the forensics investigation exists in the cloud. There are many technical ways to conduct a forensic examination in cloud environment. These ways are similar to traditional examination. In the cloud environment, there are three aspects to be considered. First, the nature of crime determines the type of the system (alive or dead) which the forensics process will be performed on. Second, to determine what took place in the cloud. Third, the availability of secure channel to collect evidences over the cloud (i.e. installed collecting client on the cloud nodes/hosts must deploy digital signature and encryption algorithms to communicate with imager device.) Traditional digital forensics has two scenarios of evidence acquisitions (i.e. live-system/powered-on-system acquisition, dead-system/powered-off- system acquisition.) In the dead system, investigators only analyze hard disk images (stored data without power.) Alive systems have the

capability to analyze more evidences to be acquired than dead systems. For the same case, more evidences (e.g., running processes) can be acquired in alive system than the dead system, as shown in Figure 1.

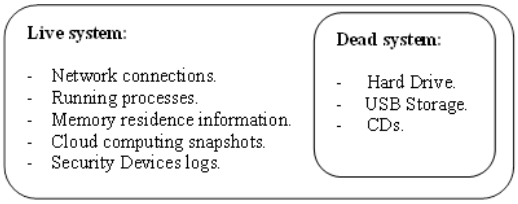

Figure 1: The relationship between both the dead and live systems.

One advantage of digital forensics in cloud environment over traditional digital forensics is that digital forensics in cloud environment is considered alive system. The cloud has valuable information and there is a possibility to be partially up, in the case of compromise. This gives the investigator more files, connections, and services to be acquired and investigated. The cloud is totally dead when shutting down the entire cloud. This possibility is almost impossible and contradicts the basic idea of cloud environment [21].

Network connection is evidence that can be acquired by alive system in the cloud environment. It is crucial to authenticate network connections to comprehend how the system communicates with others. Those connections might comprise the attacker connection to the compromised alive system. From the investigator point of view, network connection enables him/her to trace back criminal activities in the cloud environment. Investigator can link network connections to IP addresses to analyze the results with other network security devices (e.g., Firewall, IPS). This allows the investigators to (Intrusion Prevention Systems), to figure out the complete picture on how the attacker managed to connect to the compromised system. Moreover, processes running on the compromised system could be acquired from alive system. Given the pre-knowledge of the business need for the system, investigator can know programs legally installed and the running process on the system. This allows the investigator to distinguish which process is usual and which one is malicious. Furthermore, it helps the investigator to understand what changes took place on the compromised system through the analysis of the attacker's privileges and the owner of the malicious process. Also, investigator can acquire memory. This is the greatest advantage of acquiring alive system, particularly in the case of encryption is deployed. This is due the fact that encryption keys are only generated and presented in the memory. In dead systems, the running memory is gone once the power is off. The third evidence that could be acquired from alive system that uses virtualization is snapshots. It is likely to take snapshots of running machine and in the future restore and run the snapshot offline. This allows alive forensics analysis of the snapshot that comprises all process running, memory instructions, and all the connections done by the system [22-23].

Given that the security programs are hosted on the system and synchronized with the system clock. There are seven items to be acquired on a cloud system to map the digital evidence acquisition to traditional forensic evidence acquisition. (i.e. acquiring the system security packages, desktop IPS logs, firewall logs and configuration, antivirus and antimalware logs.) This process of gathering logs, for security programs, allows the investigator to figure out an idea of the system behavior. Thus, the investigator will be able to correlate different output together and conduct a timely based analysis for the compromised system. The fifth item is to acquire the guest applications running on the system. This allows the investigator to comprehend the usage and nature of the system. Moreover, it allows the investigator to inspect any abnormal application for malicious activities. Then, the investigator correlate those applications to the running process, acquired previously, to determine the application and its corresponding process [24].

Acquiring the operating system is essential to comprehend the structure and interaction between all acquired items. Unfortunately, operating system in a cloud computing systems is complex than the traditional one. Acquiring operating system in cloud computing is the sixth acquired evidence. To acquire operating system in cloud computing system, there are three components out of the cloud system to be acquired. First, acquire the guest operating system. So, the investigator will be able to discover present back doors, system accounts that have administrator rights, and system keys. Secondly, acquire the host operating system (as interpreter between the guest operating system/application and other cloud member operating system.) The third, acquire the specifications of virtualization (determine the allocated hard disk, size of memory, and network interfaces.) Seventh, acquire the cloud machine physical hard disk (using agent installed on a cloud compromised system.) This agent must encrypt and digitally sign the data before sending it through the cloud [25].

Trust in the cloud environment is very important issue. For example, assume that a computer has been manipulated to plan a murder and if law enforcement removes the hard drive for imaging. In this case, law enforcement must trust their hard drive hardware to correctly read the disk. On the other hand, if law enforcement run forensic tool on alive computer, they must trust the integrity of the host operating system in addition to the hardware. Let us assume that the compromised system is hosted in the cloud, new layers of trust are introduced. As a risk mitigation strategy, the forensic investigator should examine evidence as multiple items, as mentioned before in the seven acquiring steps. This allows the investigator to check for inconsistency and to correlate evidence. In the next section, we discuss the issue of trust in cloud digital forensics and introduce our proposed attack against Hou et al.'s scheme [3]. Moreover, we present a simple fix to prevent this attack.

6. Proposed Modification to Hou *et al.* Scheme

In [3], Hou *et al.* proposed an "encryption-then-blind signature with designated verifier" scheme to prove the authenticity and integrity of the evidence in cloud environment. Hou *et al.* aim to improve the investigation efficiency and protect the privacy of irrelevant users, one strategy is to let the server administrator search, retrieve and hand only the relevant data to the investigator, where the administrator is supposed to be responsible for managing the data in a secure manner. Due to some special crimes, the investigator may not want the administrator to know what he is looking for. In short, it is indispensable to consider how to protect both confidentiality of investigation and privacy of irrelevant users in such forensic investigation. For simplicity of description, Hou *et al.* refer to this problem as "server-aided confidential forensic investigation". When the above-mentioned relevant data is presented as evidence during a trial, Hou *et al.* aim to realize that the administrator (or the third party the administrator trusts) can verify whether the presented evidence is the data that comes from the server and whether the evidence is altered or not.

Currently, the common approach to achieve both message confidentiality and authenticity is to sign the message and encrypt it with its signature. The sender would sign the message using a digital signature scheme, and then encrypt it with an appropriate encryption algorithm. The signature would use a private key encryption algorithm, under a randomly chosen message encryption key. The random message encryption key would then be encrypted using the recipient's public key. We call this two-step approach "sign-then-encrypt" or "encrypt-then-sign" [26]. In [3], Hou *et al.* use encrypt-then-sign approach. Encrypt-then-sign is subject to the plaintext-subsection attack and it is more vulnerable when the sender uses RSA (as described by Hou *et al.* in [3]) or ElGamal algorithms for encryption and decryption [27]. The composition of the sign-then-encrypt approach suffers from a forwarding attack. On the other hand, the composition of the encrypt-then-sign approach suffers from cipher text stealing attacks.

In public key cryptography, when Bob receives a message that is digitally signed by Alice, he is assured that it was generated by Alice. This is due the fact that Alice used her private key to generate this signature. Let $C = \{M\}_{Alice}$ denote the operation of encrypting a message M with Alice's public key. Also, let $M = [C]_{Alice}$ denote the operation of decrypting a ciphertext C with Alice's private key. Since the signing and decryption operations are essentially the same, in this section, the notation for signing a message M by Alice is also denoted by $S = [M]_{Alice}$. Furthermore, the encryption operation is the inverse of the decryption operation.
Hence, $[\{M\}_{Alice}]_{Alice} = \{[M]_{Alice}\}_{Alice} = M$

In what follows, we show that the encrypt-then-sign scenario has a potential pitfall. Assume that Alice has discovered a breakthrough business idea and wants to inform her boss, Victor, about her discovery. Then, Alice will encrypt the message M using Victor's public key and then sign the result using her secret key. Then, Alice sends $[\{M\}_{Victor}]_{Alice}$ to Victor. However, Bob can set himself as a man-in-the middle and intercept messages from Alice to Victor. Bob can then use Alice's public key to compute $\{M\}_{Victor}$. Then, Bob signs it and sends $[\{M\}_{Victor}]_{Bob}$ to Victor. When Victor receives $[\{M\}_{Victor}]_{Bob}$ and verifies Bob's signature on it, Victor will assume that Bob has made this astonishing discovery and Alice cannot disprove Bob's claim.

To mitigate security breaches in the two-block approach, we present the three-block approach (i.e. Sign-Encrypt-Sign and Encrypt-Sign-Encrypt.) [28-29], Figure 2. Confidentiality, authenticity, and integrity goals can be achieved through cryptographic algorithms. Information security aims to protect the availability, privacy, and integrity of data through the use of digital signature and encryption algorithms [30]. Data

confidentiality and data integrity are two of the most important functions of modern cryptography. Confidentiality can be achieved using encryption algorithms or ciphers, whereas integrity can be provided by the use of authentication techniques. Encryption algorithms fall into one of two broad groups: private key encryption and public key encryption. Likewise, authentication techniques can be categorized by private key authentication algorithms and public key digital signatures [27]. Precisely speaking, an encryption scheme must guarantee that any information about plaintext form cipher text cannot be learned. Additionally, a signature scheme must guarantee that a valid signature on a message cannot be forged by any adversary [31-32]. Encryption algorithms can be used to protect transmitted data from one system to another over the cloud. To simultaneously achieve the security goals of encryption and digital signature schemes, different cascaded encryption and signature blocks can be used. There are two possible scenarios: Sign-Encrypt-Sign and Encrypt-Sign-Encrypt. Both of these two scenarios can resist the cipher-text forwarding attack and its consequences [32]. To ensure confidentiality and chain of custody for the digital forensics process in the cloud, Hou *et al.'* scheme (section 3.2 in [3]) needs another encryption step, at the sender side, after the "Blind signature" step (step number 2 in section 3.2 in [3]). At the recipient side, Hou *et al.'* scheme needs another decryption step after the "Signature verification" step (step number 4 in section 3.2 in [3]). These are two extra steps (one block for encryption at the sender side and one block for decryption at the recipient side) are the mitigations for Hou *et al.'* scheme against the plaintext-subsection and cipher text stealing attacks.

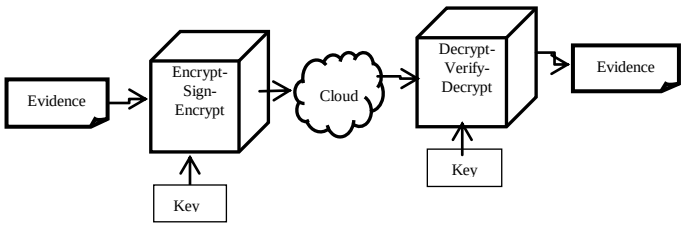

Figure 2 Block diagram of the Encrypt-Sign-Encrypt scheme

7. Conclusions and Future Work

All seven acquisition steps are mandatory to acquire evidences from a cloud computing system to complete the picture for an investigation of a compromised cloud computing system. Evidence acquisition is a challenging process in cloud environment. Thus, network plan, legal process map, clear and precise policy for each activity on the cloud computing system makes it easier to investigate a digital forensic case in that cloud environment. In this paper, we show that Hou *et al.'* scheme [3] does not preserve its claimed integrity and authenticity. Moreover, we present a modification to Hou *et al.'* scheme [3] to overcome the discovered security pitfalls.

There are many challenges for applying digital forensics in cloud computing environment. We have thousands of cloud computing systems around us. Many of these systems contain the attacker's systems. These systems might detect that there is a digital forensic investigation that takes place in the cloud. Thus, attacker may try to alter data collected by the agent installed on the compromised system, so considering an efficient strong encryption technique between the agent and the destination where the evidence is acquired should have a high priority for future work.

References

[1] S. Hou, T. Uehara, S.M. Yiu, L.C.K. Hui, and K.P. Chow, "Privacy Preserving Confidential Forensic Investigation for Shared or Remote Servers," Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2011, pp. 378-383.

[2] S. Hou, T. Uehara, S.M. Yiu, L.C.K. Hui, and K.P. Chow, "Privacy Preserving Multiple Keyword Search for Confidential Investigation of Remote Forensics," Third International Conference on Multimedia Information Networking and Security, 2011, pp. 595-599.

[3] S. Hou1, R. Sasaki, T. Uehara, and S. Yiu, "Verifying Data Authenticity and Integrity in Server-Aided Confidential Forensic Investigation," Lecture Notes in Computer Science 7804, Springer, 2013, pp. 312-317.

[4] C.N. Hoefer and G. Karagiannis, "Taxonomy of cloud computing services," GLOBECOM Workshops (GC Wkshps), IEEE, 2010, pp. 1345-1350.

[5] B.P. Rimal, C. Eunmi, and I. Lumb, "A Taxonomy and Survey of Cloud Computing Systems," NCM '09. Fifth International Joint Conference on INC, IMS and IDC, IEEE, 2009, pp. 44-51.

[6] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," Journal of Internet Services and Applications, vol. 1, 2010, pp. 7-18.

[7] S.P. Abirami and R. Shalini, "Linear Scheduling Strategy for Resource allocation in Cloud Environment," International Journal on Cloud Computing and Architecture, vol. 2, no. 2, 2012, pp. 9-17.

[8] R. Kanday, "A Survey on Cloud Computing Security," IEEE International Conference on Computing Sciences (ICCS), 2012, pp. 302-311.

[9] B. Grobauer, T. Walloschek and E. Stöcker, "Understanding Cloud Computing Vulnerabilities," IEEE Security & Privacy,vol.9, no.2, 2011, pp. 50-57.

[10] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," NIST, 2011, Special Publication 800-145.
[11] M.A. Caloyannides, N. Memon, and W. Venema, "Digital Forensics," IEEE Security & Privacy, vol. 7, no. 2, 2009, pp. 16-17.
[12] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to integrating forensic techniques into incident response," NIST, 2006, Special Publication 800-86.
[13] S. L. Garfinkel, "Digital forensics research: The next 10 years," Digital Investigation, Elsevier, vol. 7, 2010, pp. S64-S73.
[14] E. Casey, "Handbook of Digital Forensics and Investigation," Academic Press, 2009.
[15] B.D. Carrier, "Basic Digital Forensics Investigation Concepts," http://www.digital-evidence.org/di_basics.html, 2006.
[16] N. Beebe, "Digital Forensic Research: The Good, the Bad and the Unaddressed," IFIP Advances in Information and Communication Technology, 2009, vol. 306, Springer, pp. 17-36.
[17] B. Martini and K.-K. Choo, "Cloud storage forensics: ownCloud as a case study, Digital Investigation," vol. 10, no. 4, 2013, pp. 287-299.
[18] K. Ruan, "Cybercrime and Cloud Forensics: Applications for Investigation Processes," Information Science Reference, 2013.
[19] A. Saxena, G. Shrivastava, and K. Sharma, "Forensic Investigation in Cloud Computing Environment," The International Journal of Forensic computer Science, vol. 2, 2012, pp. 64-74
[20] K. Ruan, J. Carthy, T. Kechadi, and M. Crosbie, "Cloud forensics: An overview," In proceedings of the 7th IFIP International Conference on Digital Forensics, 2011, pp.16-25.
[21] R. Adams, "The Advanced Data Acquisition Model (ADAM): A process model for digital forensic practice," Murdoch University, 2013.
[22] D. Birk and C. Wegener, "Technical issues of forensic investigations in cloud computing environments," IEEE Sixth International Workshop on Systematic Approaches to Digital Forensic Engineering, 2011, pp. 1-10.
[23] J. Vacca, "Computer forensics: computer crime scene investigation," Delmar Thomson Learning, 2005.
[24] M. Sudha and M. Monica, "Enhanced security framework to ensure data security in cloud computing using cryptography," Advances in Computer Science and its Applications, vol. 1, no. 1, 2012, pp. 32-37.
[25] K. W. Nafi, T. S. Kar, S. A. Hoque and M. M. A. Hashem, "A newer user authentication, file encryption and distributed server based cloud computing security architecture," International Journal of Advanced Computer Science and Applications, vol. 3, no. 10, 2012, pp. 181-186.
[26] Y. Zheng and H. Imai, "How to construct efficient signcryption schemes on elliptic curves," Information Processing Letters, vol. 68, Elsevier Inc., 1998, pp. 227-233.
[27] C.P. Schnorr, "Efficient identification and signatures for smart cards," Advances in Cryptology - Crypto '89, Springer-Verlag, 1990, Lecture Notes in Computer Science, nr 435, pp. 239-252.
[28] M. Rasslan and H. Aslan, "On the Security of Two Improved Authenticated Encryption Schemes," International Journal of Security and Networks, vol. 8, no. 4, 2013, pp. 194-199.
[29] G. El-Kabbany, H. Aslan, and M. Rasslan, "An Efficient Pipelined Technique for Signcryption Algorithms," International Journal of Computer Science Issues, vol. 11, issue 1, no. 1, 2014, pp. 67-78.
[30] T.-Y. Wu, T.-T. Tsai and Y.-M. Tseng "A Revocable ID-based Signcryption Scheme", Journal of Information Hiding and Multimedia Signal Processing, ISSN 2073-4212, vol. 3, no. 3, 2012, pp. 240-251.
[31] D.R.L. Brown, "Deniable authentication with RSA and multicasting," Cryptology ePrint Archive, http://eprint.iacr.org/2005/056.pdf, Feb 2005.
[32] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. Information Theory, vol. it-22, 1976, pp. 472-492.

Mahmoud M. Nasreldin is a Ph.D. student at the Electronics and Telecommunication Department in Ain Shams University, Cairo, Egypt. He received his B.Sc. degree in Electronics and Telecommunications Engineering from the Faculty of Engineering, Cairo University, Egypt.

Magdy El-Hennawy is a Computer Science & Information Technology Professor at Shorouk Academy, Cairo, Egypt. He received his B.Sc. degree from the Faculty of Engineering, Ain Shames University, Cairo, Egypt. He obtained his Master degree in Performance Evaluation of Security and Integrity Measures for Database Systems from the same Faculty, as well as, his Ph.D. degree in Cryptographic Engineering for Securing Information Exchanged over the Internet. During his professional career, he was a senior engineer, deputy manager, and the manager of an Information System Centre, that is specialized in building, rolling out, operating, supporting and maintaining distributed systems over geographically distributed locations.

Heba Kamal Aslan is a Professor at Electronics Research Institute, Cairo-Egypt. She received her B.Sc. degree, M.Sc. degree and Ph.D. degree in Electronics and Communications Engineering from the Faculty of Engineering, Cairo University, Egypt in 1990, 1994 and 1998 respectively. Aslan has supervised several masters and Ph.D. students in the field of computer networks security. Her research interests include: Key Distribution Protocols, Authentication Protocols, Logical Analysis of Protocols and Intrusion Detection Systems.

Adel El-Hennawy is a Telecommunication and Electronics Engineering Professor at Ain Shams University, Cairo, Egypt.