LiveForen: Ensuring Live Forensic Integrity in the Cloud

[1]Ms. Anchana B.S, [2]Ms. Anju J.P

[1]Assistant Professor, [2]PG Scholar
Department of Computer Science and Engineering,
Marthandam College of Engineering and Technology, Kuttakuzhi, India

***Abstract*: To expedite the forensic investigation process in the cloud, excessive and yet volatile data need to be acquired, transmitted, and analyzed in a timely manner. A common assumption for most existing forensic systems is that credible data can always be collected from a cloud infrastructure, which might be susceptible to various exploits. The proposed system presents the design, implementation, and evaluation of LiveForen, a system that enforces a trustworthy forensic data acquisition and transmission process in the cloud, whose computer platforms' integrity has been verified. To fulfill this objective, it uses two secure protocols that verify the fingerprints of the computer platforms, as well as the attributes of the human agents, by taking advantage of the trusted platform module and the attribute-based encryption. The proposed framework is modeled with reversible watermarking and compression technique. To transmit forensic data as a data stream and verify its integrity at the same time, a unique watermark is embedded into the data stream without altering the data itself. While using the fragile watermarking it is crucial to restore the original image without any distortions. The watermarking techniques satisfying those requirements are referred to as 'reversible watermarking'. Reversible watermarking is designed so that it can be removed to completely restore the original image.**

***Keywords*: Liveforen, Reversible Watermarking, ABE, Forensic Data**

1. INTRODUCTION

Software as a Service (SaaS). Provides the consumer with the capability to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices, through a thin client interface, such as a web browser (e.g. web-based email). The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Four deployment models have been identified for cloud architecture solutions, described below:

- Private cloud. The cloud infrastructure is operated for a private organization. It may be managed by the organization or a third party, and may exist on premise or off premise.
- Community cloud. The cloud infrastructure is shared by several organizations and supports a specific community that has communal concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party, and may exist on premise or off premise.
- Public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- Hybrid cloud. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology, that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

Existing data integrity verification techniques, including the Checksum, Message Authentication Codes (MAC), and Digital Signature, are designed to verify the data integrity as a monolithic piece and are incapable of localizing any manipulation in a data stream. For live forensics, it is crucial and yet challenging to know the integrity of the evidence, as well as to localize any data manipulation. Any one of these challenges might defeat the forensic investigation process. The proposed system presents a novel framework that secures evidence acquisition and transmission in the IaaS cloud environment. The proposed system aims to overcome the following four research challenges (RCs) and thus makes contributions accordingly:

• **RC1**: Constructing a TCB that guarantees the integrity of the cloud infrastructure, on which a trustworthy relationship between parties can be established and maintained.

The proposed system overcome this challenge by leveraging the commodity security hardware (e.g., TPM) as the building block to support both security-critical functionalities and data integrity. Thus, it is resilient to the subversion of malicious privileged domains, OS, and firmware. Moreover, the time-consuming crypto operations are minimized to reduce performance overhead.

• **RC2**: Authenticating the human agents and enforcing the control policy to access data in the cloud. To overcome this challenge, the proposed approach enforces access control policies in the design of the secure protocols. The correctness of the secure protocols has been formally proven and experimentally verified by two formal security protocol verifiers.

• **RC3**: Verifying the integrity of evidence on the fly and keeping the integrity information accountable. The proposed approach overcomes this challenge by embedding the integrity information into streaming data groups as the fragile watermark. In such a way, any malicious data manipulation, such as insertion, deletion, and modification, can be detected and localized to the particular data groups during the real time. The verifiable integrity information will be written back to the TPM, which allows forensic data acquisition to be resumed upon future request.

• **RC4**: Developing a feasible prototype that addresses the common technical issues of a live forensic process. To do that, first compare the work with the prior solutions in the field. Then, present a prototype system, Live Integration Verifiable Environment for Cloud Forensics (LiveForen), which is deployed in the actual cloud infrastructure. The evaluation results show that LiveForen can achieve low overhead for attestation, data integrity verification, and good scalability in the IaaS cloud environment.

II. RELATED WORKS

Anyi Liu et al., proposed the two secure protocols that verify the fingerprints of the computer platforms, as well as the attributes of the human agents, by taking advantage of the trusted platform module and the attribute-based encryption. To transmit forensic data as a data stream and verify its integrity at the same time, a unique fragile watermark is embedded into the data stream without altering the data itself. The watermark allows not only the data integrity to be verified but also any malicious data manipulation to be localized, with minimum communication overhead.

Shams Zawoad et al., introduces a Secure-Logging-as-a-Service (SecLaaS), which stores virtual machines' logs and provides access to forensic investigators ensuring the confidentiality of the cloud users. Additionally, SeclaaS preserves proofs of past log and thus protects the integrity of the logs from dishonest investigators or cloud providers.

John Bethencourt et al., proposes the Attribute Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in the system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt.

John Krautheim et al., define a unique Trusted Environment Key that combines trust from the information owner and the service provider to create a dual root of trust for the TVEM that is distinct for every virtual environment and separate from the platform's trust.

Marwan Darwish et al., states that due to the nature of cloud computing, the methodologies for preventing or stopping DDoS attacks are quite different compared to those used in traditional networks. it investigate the effect of DDoS attacks on cloud resources and recommend practical defense mechanisms against different types of DDoS attacks in the cloud environment. Cloud computing is the utilization of hardware and software combined to provide services to end users over a network like the internet.

C. Chen et al., Current Trusted Platform Modules (TPMs) cTPM, an extension of the TPM's design that adds an additional root key to the TPM and shares that root key with the cloud. As a result, the cloud can create and share TPM-protected keys and data across multiple devices owned by one user. Further, the additional key lets the cTPM allocate cloud-backed remote storage so that each TPM can benefit from a trusted real-time clock and high performance, non-volatile storage. This paper shows that cTPM is practical, versatile, and easily applicable to trusted mobile applications.

Huiping Guo et al proposes a novel fragile watermarking algorithm which verifies the integrity of streaming data at the application layer. The data are divided into groups based on synchronization points, so each group can be synchronized and any modifications made to one group only affect up to two groups. A unique watermark is embedded directly into each group to save communications bandwidth. The embedded watermark can detect as well as locate any modifications made to a data stream.

III. PROPOSED SYSTEM

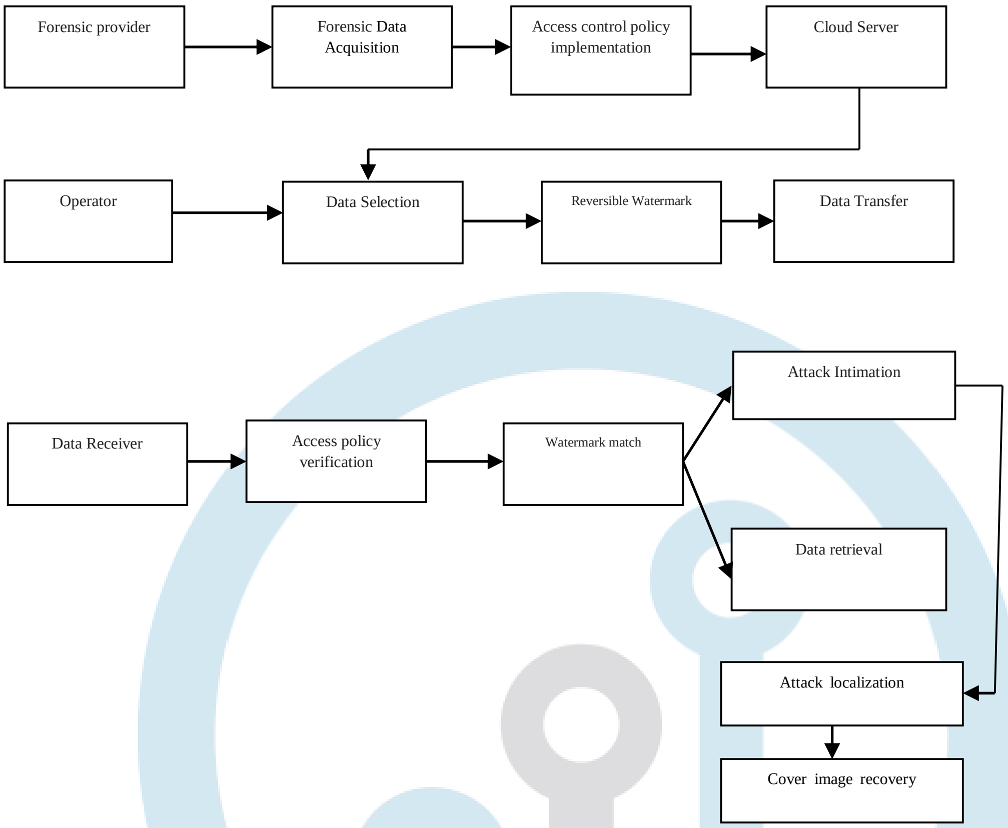

Fig 1: Block Diagram

IV. METHODOLOGY

A. Forensic provider

Forensic provider performs the data acquisition and transmission process to the cloud.The forensic provider prepares data resumption request M1 with the procedure Request_Resumption. This procedure first reads TPM to obtain the nonce ni and the last GIS saved at the end of the previous data transmission process. Then, the signed clock tick count is read from the TPM. To challenge the CP, an access control policy P is composed to include the value of GIS and nonce used in the previous transmission process, along with the current clock tick count. Finally, the message is encrypted with the public bind key BK+CP.

B. Encryption

The TPM-related, CP-ABE-related, and symmetric key-related overheads are measured. In particular, the TPM-related encryption includes the operations of 1) quoting and signing the PCR values, 2) encrypting the message with the public bind key, and 3) the generation of nonces. The TPM-related decryption overhead includes the time spent to decrypt the message with the public AIK key and private bind key. The CP-AB-related overhead includes encrypting or decrypting the message with the CP-ABE keys along with the access control policy.

C. ABE Setup: This algorithm takes as an input security parameter k, and returns public key PK which is used for encryption by sender and secret master key MK which is used by TA to generate user secret keys. Encrypt: This algorithm takes as input PK, M & T; and outputs ciphertext CT. Key Generation: It takes as an input γ associated with user & MK. It outputs SK used to decrypt message encrypted under T if and only if γ matches T. Decrypt: It takes as input CT`, SK for γ. It outputs M if and only if γ satisfies access structure associated with CT.

- Setup: The KGC generates public parameters for the whole system. Then, the KGC, output their public key and master private key pairs and respectively.
- Key Generation. . The KGC takes and a set of attributes as input, and it outputs the private key for the user.
- Data Encryption. . The data owner takes, and the tree access structure as parameters to encrypt the data object. The data owner outputs a cipher text.
- Token Generation. . The user takes and the set of attributes as input and outputs a token.

D. Reversible Watermarking

Watermarking tries to hide a message related to the actual content of the digital signal, while in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence. A reversible watermarking technique must be used to completely restore the original image after the watermark information has been extracted. The use of such a technique also enables the embedding of multiple watermarks. Embedding watermarks into the data stream might invalidate the widely accepted principle. The proposed approach does not invalidate the forensic principle for at least three reasons. First, the fragile watermark is computed from the raw data but do not alter the data itself. Since it only serves as the provable checksum that verifies the integrity of the streaming data, it can be decoupled from the evidence easily if the bandwidth is not a concern. More precisely, the GISes are still computed from the data, but are transmitted in a dedicated channel. Hence, a proper synchronization mechanism is needed to ensure that the GISes can verify their corresponding data groups on the fly. Second, as another attacker vector, a compromised data transmitter can tamper the raw evidence during the GIS embedding phase. However, as a pre-requisite to run LiveForen, the integrity of the data transmitter must be verified. Digital watermarking is the act of hiding a message related to a digital signal (i.e. an image, song, video) within the signal itself. It is a concept closely related to steganography, in that they both hide a message inside a digital signal. Watermarking tries to hide a message related to the actual content of the digital signal, while in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence. A reversible watermarking technique must be used to completely restore the original image after the watermark information has been extracted. The use of such a technique also enables the embedding of multiple watermarks

E. Verification

Data transmitter can tamper the raw evidence during the GIS embedding phase. However, as a pre-requisite to run LiveForen, the integrity of the data transmitter must be verified. A compromised data transmitter won't pass the verification and can thus be easily detected. Lastly, Grispos states that although the forensic provider can use the cloud provider's tools to verify the integrity of the evidence, the ability to validate the correctness of the tools might be limited. In LiveForen, however, the verification of data integrity depends on both parties. Data transmitter can tamper the raw evidence during the GIS embedding phase. However, as a pre-requisite to run LiveForen, the integrity of the data transmitter must be verified. A compromised data transmitter won't pass the verification and can thus be easily detected. Lastly, Grispos states that although the forensic provider can use the cloud provider's tools to verify the integrity of the evidence, the ability to validate the correctness of the tools might be limited. In LiveForen, however, the verification of data integrity depends on both parties. That is, the nonces (n3 and n4) used to determine the group size are generated by the CP and the FP, respectively. Therefore, the ability of validating the correctness of the data depends on both custodians and thus is not limited.

F. Error localization and recovery

The proposed scheme can realize not only tamper detection and localization but also tamper recovery. Moreover, tamper recovery is based on block division and the recovery accuracy varies with the contents that are possibly tampered. The received image is transformed into Discrete Wavelet Transformation (DWT) domain and divided into important part, that is, low-frequency part, and unimportant part, that is, high-frequency part. Then, different parts are processed differently to realize different goals. Since the low-frequency part contains the main information of image, traditional chaotic encryption is employed in encryption stage so that the low-frequency part can be fully recovered in decryption stage. Then, for the high-frequency part, Compressive Sensing (CS) is used to conduct encryption so as to vacate space for watermark embedding. The scheme takes the processed content of original image as watermark, from which the characteristic digest values are then generated. The watermark is designed mainly for tamper recovery while the digest values are considered as the standard of tamper detection.

CONCLUSION

The proposed system is an acquisition and transmission in an IaaS cloud environment, a novel framework that allows forensic evidence to be acquired and transmitted between trusted platforms is presented. Forensic data are transmitted as streaming data, in which the data integrity information is generated as the fragile watermarks. The benefits of using the watermarks allow custodians to verify the data integrity, as well as detect and localize malicious modification at run time. To transmit forensic data as a data stream and verify its integrity at the same time, a unique watermark is embedded into the data stream without altering the data itself. While using the fragile watermarking it is crucial to restore the original image without any distortions. Reversible watermarking is designed so that it can be removed to completely restore the original image. The prototype of the system has been implemented in an IaaS cloud environment, whose security properties have been proven by formal security protocol verifiers.

REFERENCES

[1] S. T. King, P. M. Chen, Y.-M. Wang, C. Verbowski, H. J. Wang, and J. R. Lorch, "SubVirt: Implementing malware with virtual machines," in Proc. IEEE Symp. Secur. Privacy, May 2006, pp. 314–327.

[2] V. Ciancaglini, M. Balduzzi, R. McArdle, and M. Rösler. (2015). Below the Surface: Exploring the Deep Web. [Online].

[3] Symantec. Avoiding the Hidden Costs of the Cloud. Accessed: Aug. 1, 2018. [Online]. Available: https://www.symantec.com/content/ en/us/about/media/pdfs/b-state-of-cloud-global-results-2013.en-us.pdf [4] R. Samani and F. Paget. (2013).

[5] M. Darwish, A. Ouda, and L. F. Capretz, “Cloud-based DDoS attacks and defenses,” in Proc. Int. Conf. Inf. Soc., Jun. 2013, pp. 67–71.

[6] D. Goodin. ZeusBot Found Using Amazon’s EC2 as C&C Server. [Online]. Available: ttp://www.theregister.co.uk/2009/12/09/amazon_ec2_bot_control_channel/

[7] M. D. Ryan, “Cloud computing security: The scientific challenge, and a survey of solutions,” J. Syst. Softw., vol. 86, no. 9, pp. 2263–2268, Sep. 2013.

[8] D. Zissis and D. Lekkas, “Addressing cloud computing security issues,” Future Gener. Comput. Syst., vol. 28, no. 3, pp. 583–592, Mar. 2012.

[9] NIST Information Technology Laboratory. (2013). NIST Cloud Computing Forensic Science Challenges. [Online]. Available: http://csrc.nist. gov/publications/drafts/nistir-8006/draft_nistir_8006.pdf

[10] U. S. Congress. (2018). Cloud Act. [Online]. Available: https://www. congress.gov/bill/115th-congress/house-bill/4943

[11] (2017). Forensics at the OJ Simpson Trial. [Online]. Available: https://www.crimemuseum.org/crime-library/famousmurders/forensicinvestigation-of-the-oj-simpson-trial/