SIDNFF: Source Identification Network Forensics Framework for Cloud Computing

Suleman khan, *Student Member, IEEE,* Abdullah Gani, *Senior Member, IEEE,* Ainuddin Wahid Abdul Wahab, Mustapha Aminu Bagiwa, *Member, IEEE*

***Abstract*— This paper presents a novel framework for network forensics in cloud computing (CC). The framework investigates malicious activities performed by an intruder while affecting virtual machine on same or another cloud resource (CR). Moreover, it investigate malicious activities of intruders by determining its source while keeps privacy for cloud users with out losing their data confidentiality. Our proposed framework provides initial foundations to create real network forensics model for CC in a right essence.**

INTRODUCTION

The easy access, low cost, transparent application execution, high computational resources, less configuration, and quick output assist users to adopt the services of CC [1-2]. However, with such services, it opens a gateway for malicious users to have an access to CC for performing different vulnerabilities [3]. Vulnerabilities could be in form of DDoS attacks, data breaches, service traffic hijacking, API attacks, and malicious inside users [4]. The important aspect for aforementioned vulnerabilities is to identify the source of the attack to prevent them in the future [5].

In this paper, we have proposed a source identification network forensics framework (SIDNFF) for CC to identify malicious users by investigating their activities in virtual machine (VM) and network record. The proposed framework is in preliminary implementation stage and will be evaluated in Open source CC development environment such as Open Stack.

PROPOSED FRAMEWORK

The proposed framework is used to identify malicious activities of an intruder performed on VM of its own or another physical CR. The source of an intruder is identified without compromising innocent user's data. The main components of our proposed framework SIDNFF is as follows.

A. Cloud Computing User Interface

Cloud Computing User Interface (CCUI) is a client side cloud interface of the SIDNFF framework. Its main task is to connect cloud users (CU) to CC. The CCUI provide gateway for CU to send their application to cloud for different services including storage, computation, analysis, and various others. Each CU has been assigned a unique ID to differentiate it from another user and keeps its record in a CC for further investigation purposes.

B. Cloud Computing Manager

Cloud Computing Manager (CCM) is a main component of SIDNFF to trace malicious CU in CC. Each CU is registered with CCM upon their unique ID. The CCM maintain a table known as User Identification Table (UiT) to keep record of each CU such as CU ID, assign CR and VM, its application ID, and execution time of application.

C. Cloud Computing Resource Manager

Cloud Computing Resource Manager (CCrM) is responsible to keep record of each VM of CRs in CC. The record includes VM-ID, number of application running on VM, application execution time, and VM availability. The CCrM assist CCM in identifying appropriate VM for CU application and provide useful information in investigating CU activities by providing useful information such as VM migration, attempting other VM on same or another CR, and time of attempt.

D. Cloud Computing Network Forensics Manager

Cloud Computing Network Forensics Manager (CCnFM) is responsible to perform analysis on record retrieve from Virtual Machine Monitor (VMM) and CCM. The CCnFM further pass the analysis report to cloud forensics investigators for their necessary actions.

E. Virtual Machine Monitor

Virtual Machine Monitor (VMM) is a program to provide multiple execution environments for multiple users on single CR at the same time. It monitors and records each VM activities such as new application assignment, complete execution of an application, number of applications, and application migration.

F. Working

The goal of proposed framework SIDNFF is to identify malicious user in CC by attempting to perform malicious activity on VM of CR. The malicious activity could be any action to affect CC security level such as leaking out user's data, sending extraneous messages, and various others. The SIDNFF is shown in the Figure-1, which includes all main components which is explained in the aforementioned paragraphs.

When a CU connects to CC through CCUI, it assigns a unique ID to a CU. The whole process is transparent and invisible to a CU while he/she only enters username and password assigned by cloud vendor. The CCM create a User Identification Table (UiT) upon each CU registration with CC. When suppose CU what's to execute its application on CR, the application ID is recorded with its CU-ID in a UiT. Next, the CCM request CCrM for appropriate VM on CR. The CCrM

978-1-4799-8745-0/15/$31.00©2015 IEEE

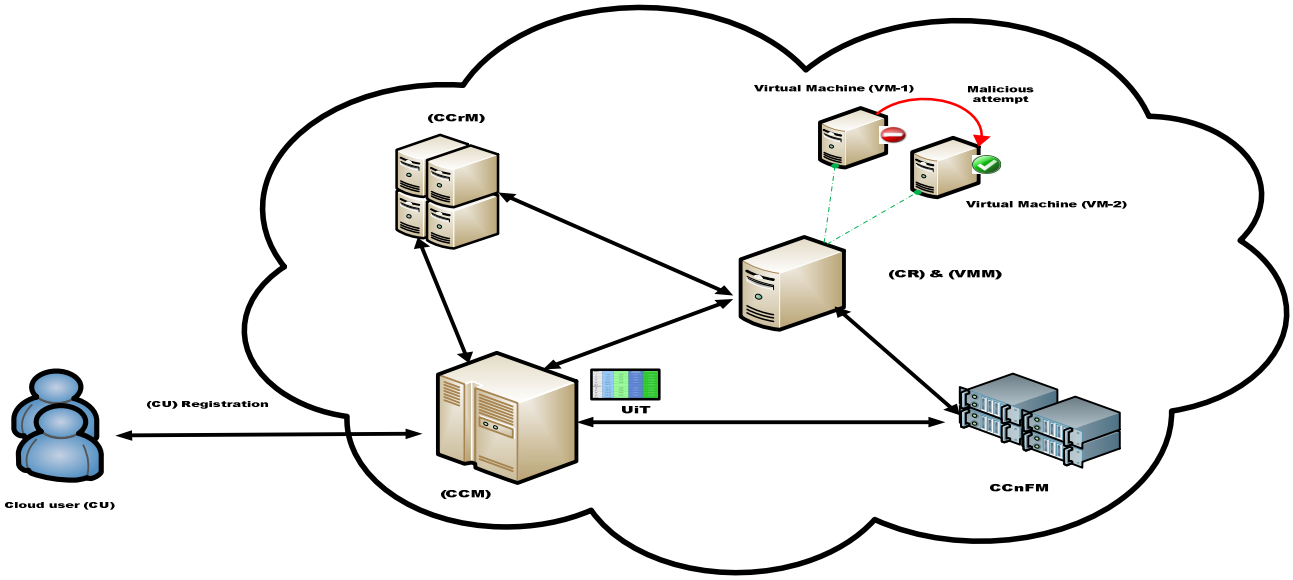

Fig. 1. The proposed framework SIDNFF

records every CR which is added or remove from the CC infrastructure such as CR IP and MAC address, number of VMs, each VM IP and MAC address, number of application executing on each VM, and each application ID. When CCrM provides information regarding CR to CCM, CCM assign CU application to a potential VM on CR and record its information in a UiT i.e. VM MAC address and application ID with its corresponding CR.

As an example, if CU application starts performing malicious behavior on its assigned VM i.e. attempts to exploit its neighbor VM on the same or another CR. Such situation is considered as suspicious due to illegal access to data of innocent CU on another VM. To track the malicious activity by identifying source of the attack is the primary task for SIDNFF. To achieve such objective by SIDNFF, VMM sends an alarm message to CCM and CCrM. The VMM send information to CCrM that includes VM IP and MAC address where malicious application is executing, malicious application ID, and time of malicious attempt on VM. The CCrM updates its record and forward the information to CCM. The CCM identifies associated user for respective malicious application and forward updated information to CCnFM. The CCnFM start analysis by investigating VM logs retrieve from VM through VMM and information send by CCM. The CCnFM retrieve useful evidence for logs by applying various network analysis tools such as Xplico [6] or various others. The evidence is verified with recorded information in UiT at CCM. The SIDNFF helps investigator to perform investigation without violating privacy issues of other CU on same or other VM.

G. Assumptions

SIDNFF makes the following assumptions:

- Each CU will assign a unique CR virtual machine which will not be changed upon VM upgrade, restart, and migration.
- CU application on VM has access to any VM in CC for performing its malicious activities.
- Information send to CCnFM is in secure way. No intruder can exploit information send between CCnFM and CCM, VMM and CCrM, and CCrM and CCM.

CONCLUSION

In this paper, we proposed novel framework for source identification of an intruder in cloud computing. The proposed framework SIDNFF facilitates cloud forensics investigator to know about intruders without affecting innocent cloud user's data such as data privacy. Moreover, it will help cloud service providers to implement such framework in their cloud infrastructure to track malicious user activities while attempting to exploit virtual machine on same or another cloud resource. In future, we are going to validate the framework through petri-nets and will implement it in Open Stack cloud development environment.

REFERENCES

1. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin and I. Stoica, "A view of cloud computing," *Communications of the ACM*, vol. 53, no. 4, 2010, pp. 50-58.
2. S. Khan, E. Ahmad, M. Shiraz, A. Gani, A.W.A. Wahab, M.A. Bagiwa, "Forensics Challenges in Mobile Cloud Computing," International Conference on Computer, Communications, and Control Technology (I4CT), 2014, pp.343-347; doi: 10.1109/I4CT.2014.6914202.
3. S. Khan, M. Shiraz, A.W. Abdul Wahab, A. Gani, Q. Han and Z. Bin Abdul Rahman, "A Comprehensive Review on Adaptability of Network Forensics Frameworks for Mobile Cloud Computing," *The Scientific World Journal*, vol. 2014, 2014, pp. 27; DOI 10.1155/2014/547062.
4. N. Gruschka and M. Jensen, "Attack surfaces: A taxonomy for attacks on cloud services," *Proc. Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on*, IEEE, 2010, pp. 276-279.
5. S. Lee and C. Shields, "Tracing the source of network attack: A technical, legal and societal problem," *Proc. Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*, Citeseer, 2001.
6. "Open Source Network Forensic Analysis Tool (NFAT)," *Xplico*, 2014.