International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

A Study on Reconstruction Methods and Approaches

Reshma Raj K S[1], Raj Kumar T[2]

[1, 2]Department of Computer Science and Engineering, College of Engineering Kallooppara, Kerala

Abstract: ***The alarming rate of digital usage and the crimes raises the need for more concentrated investigations, security policies and control measures. Any actions that result in a cause for crime or violations of the laws and policies are considered as a crime. Even if an investigator conducted his investigation but fails to produce the evidence properly then we cannot say that his investigation is completed. Another problem is the lack of measures and investigation tools for the distributive environment such as cloud systems. Many challenges faced in this systems are large storage, remote data collection, physical inaccessibility etc. And here in this paper another challenge that is crime scene reconstruction and the existing methods for such are discussed.***

Keywords: forensics, cloud systems, events, digital investigations, crime scene reconstruction

1. Introduction

Digital forensics, sometimes known as digital forensic science, is a branch of forensic science which includes the recovery and investigation of material found in digital devices, often in relation to crime. Digital forensics investigations have a variety of applications. The most common is to support or refute a hypothesis before criminal or civil (as part of the electronic discovery process) courts. Cloud systems are one of the most efficient and pay per use model computer paradigms that are widely used nowadays. The present cloud computing architectures are insufficient in cases of security and forensics. Its dynamic nature presents researchers a new area of research known as „Cloud Forensics". These highly scalable facilities in cloud can be misused by malicious users to perform attacks from the systems within the cloud system. This will hide himself and his activities from his personal system and can even confuse an investigator. Another important thing is that a crime is not a single process. It may include a sequence of actions and different causes. Each of these actions is normally called as events. So reconstructing a crime includes the reconstruction of each of the events.

Our typical investigation phases are a little bit impractical in several cases of cloud systems and so is the reconstruction. But the reconstruction cannot be avoided in many situations in order to prove a case. It is sometimes inevitable to recreate the scene of what actually happens in a system and what are the changes which happens or causes the changes in the system. This process of recreating a crime by an investigator or an authorized person is called crime scene reconstruction

2. Digital Investigation

An investigation is a process of collecting evidences as well as informations, preserving these evidences, examining and analyzing and finding who, what, how and when something had happened regarding a crime or an action. The same is that of in a digital investigation slightly rather than physical evidences, digital evidences are considered. But collecting digital evidences from physical accessible machines and surroundings is also considered as a part of the digital investigation.

In normal digital investigations the first action performed by an investigator is to seize the system which is considered to be the platform for a particular crime. This can be performed as dead analysis or live analysis. Then he tries to collect informations useful for his case. From these the relevant informations are gradually considered as evidences. He then analyses the evidences and find out suspect and his motive behind the crime. He then produces these informations and conclusions as a report before a court or an authority who assigns him for the case. So in a typical digital investigation the following steps are involved:

- Collection
- Preservation
- Analysis
- Presentation.

3. Typical Investigation Vs Investigation in Cloud

Many of the assumptions of traditional digital forensics are not valid in the cloud computing model. One of the major hurdles is that neither users or nor investigators have physical access to the cloud. In cloud each servers contains different files from many users. So without violating the privacy policies of a user it is infeasible to seize servers. Another challenge is the reliability of the evidences as the data is provided by CSP"s (Cloud Service Provider) which is a third party. There is no specific method to ensure the integrity of the data. In order to provide services on demand cloud doesn"t support persistent data storage in case of terminated virtual machines (VM). So the data from cloud VM"s are not available in such cases. Other challenges are multi-tenancy, large bandwidth, logging and standards. Besides these challenges cloud has some advantages over traditional forensics like large data storage, huge computational performances, availability of resources, computation available through VM"s, easiness of acquisition, preserving, cryptanalysis and copying and transferring of data

4. Existing Reconstruction Methods and Tools

As already mentioned a crime is not a single process but sequences of events. So reconstructing each event is a modular part in crime scene reconstruction. Brian D. Carrier and Eugene H. Spafford proposed an approach;

- Role based event reconstruction
- Research by Liao and Langweg proposed another model
- Resource based event reconstruction.

4.1 Role Based Event Reconstruction

For the examination of the evidences tools must be needed in case of digital investigation which may or may not be needed in physical investigation. This can result in the difficulty of analysis but at the same time the automation of some of the procedure can be easier while using these tools.

An event can be of any type. Some can be a cause for an incident while others can be an effect of an incident. Some events even can be of no effects and these can be ignored when the investigation becomes more concentrated. In other words we can say that an event is an occurrence which can affect the state of a system or information. This event can sometimes be an object which initiates another event. These interested objects or events are collected and their characteristics are studied. The initiator object is difficult to identify in many cases. There can be one or more initiators in some cases.

Another thing to be concerned is that an investigator cannot find out all of the steps which are continuously performed by the criminal in earlier stages. For a continuous process he is only able to find out some of the discrete steps or events and some of them are through his assumptions. This is because some of the events can occur at the same time while some can be on discrete time.

An event chaining is a sequence of events that can cause one after the other or we can say if event e_i is a cause for e_{i+1} and the series of events e_i for which i= 0,1,...K for k events. In their reconstruction process they describe about 5 phases. They are:

1) Evidence Examination
2) Role Classification
3) Event Construction and Testing
4) Event Sequencing
5) Hypothesis Testing

In the first phase their main objective is to identify relevant objects and its characteristics. An object can have 2 properties; individual as well as class characteristics. Individual properties include unique characters that it has and class properties are those characteristics which are common with other objects.

In the role identification phase some of these individual objects can be considered as initiators which either exhibit as a cause for an event. Also the events that are an effect of an event is also filtered out. Now we get 2 classes of objects cause objects and effect objects.

In the next phase we continuously construct and test our causing objects and effects. This can be time consuming and erroneous. Sometimes in this phase we may end up in searching for further objects. For the missing roles and objects hypothesis is created and tested. This is repeated for all the events.

In the event sequencing phase they are trying to correlate each of these events into one single process or event chains. The time stamp and other temporal informations help to sequence these events easily. In other cases several another sequencing techniques like relational and functional informations.

4.2 Resource Based Reconstruction

This is similar to that of pole based except that it may contain a readiness phase for the evidence admissibility. It has the following phases:

- Readiness for collecting system call traces
- Deployment phase for receiving detection alerts
- Investigation phase for preserving and recognizing evidences
- Reconstructing events

This approach basically focuses on pre-detecting crimes.

Another automated approach for crime scene reconstruction at higher levels is done through an automated timeline reconstruction framework. The high level reconstruction is performed with the help of forensic tools along with pattern matching and human understandable events.

Here the high level reconstruction is done through the following steps:

1) Initially retrieve the preserved data to collect informations
2) Clustering or grouping of data with similar functionalities.
3) Searching within these clusters for possible events.
4) Similarity measure is performed.
5) Reporting the event.

The main advantage of this model is that it helps the investigator to identify possible causes for his hypothesis from the characteristics and properties shown by the potential evidences.

4.3 Database Reconstructions

This includes normal methods which are performed during any transactions. When a transaction is aborted then all the events related to that particular transaction is roll backed to the previous consistent state. Any changes to the database can be easily roll backed by aborting the transactions.

5. Conclusion and Future Scope

The paper discusses about the existing scenarios for event reconstruction. In case of cloud systems a single framework or tool is developed for the process. The paper tries to prove that the existing methods rely mainly on event reconstruction which can be further extending for the crime scene reconstruction. Many of the forensic tools mostly

focus on data collection and analysis. So the need for an efficient reconstruction framework or tool is on urge.

References

[1] Carrier B, Spafford EH, defining event construction of digital crime scene, Forensic Sci, Nov. 2004, Vol. 49, No. 6.
[2] S Zawoad, R Hasan. ―Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems‖. ArXiv preprint 2013S.
[3] Victer R Kebande and HS Ventor, "Adding event reconstruction to a cloud forensic readiness model," IEEEjournal.

Author Profile

Raj Kumar T graduated the degree of Master of Technology from National institute of Technology Karnataka Surathkal and is presently working as Assistant Professor in Computer Science and Engineering at College of Engineering Kallooppara.

Reshma Raj K.S graduated the Degree of Bachelor of Technology in Computer Science and Engg. from College of Engineering, Kottarakkara in 2014. She is now pursuing her master degree in Computer Science with specialization in Cyber Forensics and Information Security at **College** of Engineering Kallooppara under Cochin University of Science and Technology.