Digital Forensics Analysis in the Distributed Data Environment

[1]Mr.Jibin N and, [3]Dr. E.J. Thomson Fredrik

[1]Research Scholar, Department of Computer Science, Karpagam Academy of Higher Education,
Coimbatore - 641 021.
[2]Professor, Department of Computer Applications, Karpagam Academy of Higher Education, Coimbatore-641 021
Email: [1]jibintcr@gmail.com, [2]thomson500@gmail.com

ABSTRACT

The rate of cybercrime has increased because of the extensive use of the internet-enabled technologies. Due to the data storage of distributed services and the location of data servers in various countries, establishing methods to track the records of cyber crimes are quite difficult. The major problem in the current scenario is the legal compliance such as jurisdiction of the data servers located in various continents. The cloud servers are normally distributed all over the world to prevent the data loss due to natural disasters etc. and it is very difficult to get the details of the various events happening at different places. This paper examines the research works of various researchers on tiered approach of cyber forensic in distributed environment. This paper analyses the identification mechanisms for various types of cybercrimes and control measures of government rules and regulations to control cybercrimes. This paper reviews the cyber security problems arise due to the ongoing establishment of IoT based network and the implementation of smart cities.

Keywords: Cyber Forensics, Cloud, incidents, data mining, datadriven, discovery, machine learning, prediction.

1. INTRODUCTION

There is huge increase in the rate of digital crimes because of the wide use of internet-enabled technologies. The new forms of cyber-attacks end up in personal and organization loss of Information Technology assets. Due to the data storage using the data-distributed services, establishing the methods to track the records of theft is quite difficult due to the distribution of data servers in various countries. The major problem in the current scenario is the legal compliance such as jurisdiction of the data servers located in various continents. The legal formality to enable the review process itself is different in various countries.

One of the distributed services in high demand is cloud computing and the technology has got wide acceptance because of its boundless features and facilities such as "*as a service"*. The cloud servers are normally distributed all over the world to prevent the data loss due to natural disasters, and it is very difficult to get the details of various events happening at different places. Digital evidence that is required to be presented before a court is prepared with the help of Computer Forensics. The investigation of the content and the analysis phases are considered critical ina forensics procedure.

II. BACKGROUND

The digital Forensics techniques like analysis and review will help the investigators get evidence from the victims of targeted system to present before court. The examination of the victim system and its analysis are considered to be the most important phases of a digital forensics procedure. A brief study of literature in the cyber forensics investigation process is discussed below.

A. INTRODUCTION ABOUT CYBER FORENSICS

In [1], Mr. Nan Sun and Mr. Jun Zhang, 2019 in his paper discussed the Cyber forensics as the application of data analytical techniques in electronic data storage for legal purpose and the interpretation of the data recovered. There is huge increase in the rate if digital crimes because of the wide acceptance of internet enabled technologies by the society which ultimately results in the personal and organization loss of Information Technology assets. A wide variety of cyber-crimes activities can be properly marked by examining the digital information using the computer forensics conceptions. This information can be submitted to audit and trial court. These results obtained by a cyber-analysis will be useful to prevent future cyber-crime activities

When a cyber-crime occurs, the cyber forensics analyzers will physically isolate the device and make sure that the device is not contaminated. The digital medium where the crime occurs is made safe by creating a separate copy of it. Once the digital copy is ready then, the original medium is locked and all the analysis works are done in this copy only. In [2], M. A. Kuyperset et al., 2017, stated that the analysis included searching hidden folders and unallocated disk space to find out the deleted files, and any evidence found would be documented in a “finding report” to be submitted to the court. A basic set of activities in a cyber-forensic analysis is described below:

1) IDENTIFICATION

In the digital investigation process, the investigator should have a clear idea about the type of evidence sought and how to preserve it. He needs to study the case carefully and identify the requirements like source of information and integrity of the information to go forward to get evidence in the case. This is known as the identification phase. The integration of computation and physical processes will lead to the making of Cyber-Physical Systems. These systems are connected to internet and controlled by the distance user. If such Cyber physical systems are involved in the crime, identification mechanisms should be considered in the investigation process of cyber crimes.

2)EVIDENCE ASSESSMENT

In [2], M. A. Kuypers, et al., 2017 explained how evidence assessment can be made. All the possible sources like target system, networks, hard drives, and social media accounts are examined to retrieve information. This information is then evaluated.

3.EVIDENCE ACQUISITION AND PRESENTATION

In [4] C. Blackwell, 2010 talked about how to acquire evidence and presented it. The system involved in the crime is removed from the network and made write-protected using digital technique to ensure that no alteration is done to the evidence. The investigators ensure that the system involved in the crime activity is presented without any alteration.

4) EVIDENCE EXAMINATION

In [18], P. Bednar, 2000, presented how the agents typically examined the cyber-crimes. The cyber expert investigators would use high end digital dedicated tool to examine the data. The deleted or altered information would be identified and converted to digital evidence.

5) DOCUMENTING AND REPORTING

In [6], Kraemer, S, et al., 2009, explained how records could be created and accurately presented using cyber analysis investigation. The records created by the investigators must contain all the details about the case. The evidence is stored in archives to ensure the validity of the findings.

B. CYBER-CRIME INVESTIGATION FRAMEWORK

In [5], Mr. Jonathan McClainet et al., 2015 in their paper argued about the need of cyber-crime investigator to connect with multiple levels of officials in order to take strategic decisions. Strategic Thinking Framework (SST) must be used to capture relevant information which should be converted to the format compatible with the investigation process. With the aid of various concepts like evidence bags, automated logging-network tools etc. this could be made as a specialized system fortified for investigation.

C.GOVERNMENT REGULATIONS IN CYBER SECURITY

In [3], Jangirala Srinivasaet et al., 2019 said that it is required to compel the companies and other IT organization to follow the regulations for cyber activities for the purpose of shielding data from cyber-attacks. Several possible attacks may happen to a system in the network. As result it is required to establish or ensure numerous principles in cyber defense. A Cyber Incident Management frame work should include major components such as the technology used, security algorithms, and emergency response against cyber-attacks.

D.CYBER INVESTIGATOR PROFICIENCY FACTORS IN ANALYSIS

In [11], D'Amico et al., 2005 said that Proficiency of cyber security investigator was a major problem in this area. Proper research in the cyber forensics area should be conducted where data collection was an important aspect. This data should be properly analyzed so that future attacks could be analyzed and effectively prevented. In [7], Forsytheet et al., 2013, proposed that in order to carry out the accurate cyber forensics, the investigator should be trained and equipped with the latest technology. FIRE (Forensic and Incident Response Exercise) platform developed provides various forms of training in the digital forensics analysis activities. The ultimate objective of this model is to equip the cyber forensic investigator with the right tool.

E.SMART CITIES AND CYBER SECURITY

In [13], A.A. Cardenas et al., 2008, in their research paper stated that IoT-based smart cities would revolutionize people's lives. Smart cities heavily depend on technologies and hence probabilities for cyber-attacks could lead to significant loss. By the application of regulatory frame work for cyber security, we can ensure that security is observed. In [12],V.R. Kebande, 2016 discussed the role of cyber-framework in securing IoT-based smart cities and the network of IoT enabled devices. The framework considered the Government as policy setter and acted as coordinator in order to define and dictate the technical standards and other requirements. New economic and social opportunities are generated by the emergences of smart cities that are supported by the latest technologies like IoT, Blockchain and CPS, artificial intelligence systems etc. These new trends and innovations will lead a threat to our privacy and security. These systems will lead to unique progresses to the excellence of our life. These systems can be used in many areas of the human life. The introduction of such a framework encourages collaboration in a secure way so that effective and innovative smart cities can be built. In [14],E.A. Lee, 2018 analyzed the importance and usage of cyber physical systems and their design aspects. The researcher also stated the cyber security challenges have to be considered, when we design such systems.

F.CYBER FORENSICS IN IOT DEVICES

In [15], C.W. Tien et al., 2007 in their paper anticipated **Cyber physical Systems** and their operations in diverse situations and connects with a varied set of equipment and networks. These heterogenic, diverse, and complex systems introduced new level of vulnerabilities and need security including digital forensic capabilities. A digital forensics investigator uses the attacker's computer to catch more details and signs of the attack which may help to prove the case. In [8], Reed, T et al., 2014, presented that information regarding the attack could be extracted from the RAM. RAM artifacts of Java program can be used to extract these details. JVM runs on various platforms and the details about the program, even after the usage of garbage collector and termination of the program, can be accessed and will be helpful for an investigator. This helps the investigator to categorize the software used to takeoff the attack and understand the inner drifts. In [19], Washburn Det al.,2010, presented that the Cyber physical systems were the result of assimilation among internet technologies and physical processes which may distress the physical developments and vice versa. The machines that are used for these cyber physical systems can be easily compromised and hijacked. This mandates the need of safety measures and cyber forensics skills. Therefore, obviously the behavioral analysis will lead to the actual understanding of the persons involved in the crime.

G.BEHAVIORAL EVIDENCE ANALYSIS INTO CYBER FORENSICS ANALYSIS

In [17], G.Grispos et al., 2017 said that the Behavioral Evidence Analysis (BEA) within the computer forensics examination had limited adoption in the field. This (BEA) model takes a multidisciplinary approach which includes the investigation of the seized machines related to different cases that include details of both the offenders and the victims. This model helps to concentrate on the exploration process and logical guidelines and conclusions for the case investigation. BEA includes current practices used in Digital forensics and also other technical examinations specific to BEA. As a future work, it is required to add more capabilities to the cyber forensics using BEA. The Equivocal forensic is used in the Behavioral Evidence analysis. The first one refers to the inspection, analysis and evaluation of the evidence, and employing perilous thinking and logical analysis and the latter refers to the characteristics of the victims and analyzing to reach in conclusion.

III. CHALLENGES IN CYBER FORENSICS ANALYSIS IN THE DISTRIBUTED DATA ENVIRONMENT

The major problem in the current scenario is the legal compliance such as jurisdiction of the data servers located at various continents. The legal formality to enable the review process itself is different in various countries. One of the highly demanding distributed service is cloud computing and the technology got a wide acceptance because of its boundless features of availing facilities “as a service”. The cloud servers are distributed all over the world to prevent the data loss due to the natural disasters etc., and it is very hard to get the details of the various events happened at different instances.

IV. TIERED APPROACH FOR CYBER FORENSICS IN THE DISTRIBUTED DATA ENVIRONMENT

In this connected world, it is more effective to keep the stamp of various events happening in the environment. In [20], Joe Haggerman et al., 2017 explained the concept of tiered approach for cyber forensics. This research work may be extended to develop a novel model for a computer forensic investigation of varied big data, and it will help the examiner to identify the threat. The proposed model is composed of four steps: application analysis, operating system analysis, transaction analysis and forming an opinion. The model is independent of operating system and the application. For all transactions the model keeps a stamp of it and keeps all the details of the transaction where they occur.

A. FUNCTIONALITIES

In [9], R.G., McClain, J et al., 2015, explained the concept of application analysis when a cybercrime occurs. The Application analysis will analyze the application and help to get an initial view about the event. The module will analyze the browser artifacts relating to the events and keep a copy of the whole scenario. In [10], Stevens-Adams, et al., 2017, established the need of Operating system analysis for cyber incident prediction. The operating system analysis will identify the details of the system where the event actually happened and it keeps track of the systems that are involved in the event. In [16], J. Gosling, B. et al., 2015, explained the transaction and their management concepts for cyber incidents. The Transaction management will keep the details of the transaction such as the parties involved and other related information. A stamp of the various events in the crime is stored from these layers; this stamp can be used as an evidence for the occurrence of events.

B. CRIMINAL PROFILING

In this criminal profiling, the digital profiles of criminals are created, which will help in the investigation of the cyber-crimes. In the digital profile, the different characteristics of the criminal are identified and stored in a data warehouse. It will help in future investigation process. The criminal profile of a person includes the nature of crime scene, the details of the offense committed, and the way by which it was committed. There are two different ways for criminal profiling inductive and deductive. The inductive method uses statistical tool and methodologies to study the behavior of the criminal and this physiological devours and crime patterns are identified. In deductive methodology the profile created based on examining the type of systems and how the manner by which the crime was happened.

V. CONCLUSION

In this research paper, we discussed the various research works in the area of cyber forensics in the distributed environment. Based on the study of previous research works, we have planned to develop a novel model for digital or computer forensic analysis of dissimilar big data for helping the investigator to identify the perpetrator. The proposed model is composed of four steps: application analysis, operating system analysis, transaction analysis and forming an opinion. The model is independent of operating system and the application. The model keeps a stamp for all transactions about when and where it occurred. This model will help to analyze the cyber-crime incidents and can be used as an evidence in the investigation of cyber crimes.

REFERENCES.

[1] Nan Sun, Jun Zhang, Senior Member, “Data Driven Cyber security Incident Prediction: A Survey”, IEEE Communications Survey & Tutorial, Volume: 21, Issue: 2, Second quarter 2019.

[2] M. A. Kuypers, T. Maillart, and E. Pate-Cornell, “An Empirical Analysis of Cyber Security Incidents at a Large Organization”, Dept. Manag. Sci. Eng., Stanford Univ., Stanford, CA, USA, and School Inf., Univ. California at Berkeley, Berkeley, CA, USA, 2016.

[3] Jangirala Srinivasa, AshokKumarDasb, Neeraj Kumarc, “Government regulations in the cyber security: Framework, standards and recommendations”, Future generation computer systems 92 (2019) 178-188

[4] C. Blackwell, “A secure ontology for incident analysis,” in Proc. 6th Annu. Workshop Cyber Security Inf. Intell. Res., 2010, p. 46.

[5] Jonathen McClain, Austin Silva, Glory Emmanuel, Benjamin Anderson, Kevin Nauer, Robert Abbott and Chris Forsythe “Human Performance Factors in Cyber Security Forensic Analysis”, 6th International Conference on Applied Human Factors and Ergonomics (AHFE 2015) and the Affiliated Conferences, AHFE 2015

[6] Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. Computers & Security, 28(7), 509-520.

[7] Forsythe, C., Silva, A., Stevens-Adams, S., & Bradshaw, J. (2013). Human dimension in cyber operations: Research and development priorities. In Foundations of Augmented Cognition (pp. 418-422). Springer Berlin Heidelberg.

[8] Reed, T., Abbott, R., Anderson, B., Nauer, K. & Forsythe, C. (2014). Simulation of workflow and threat characteristics for cyber security incident response teams. Proceedings of the 2014 International Annual Meeting of the Human Factors and Ergonomics Society, Chicago, IL

[9] Abbott, R.G., McClain, J., Anderson, B., Nauer, K., Silva, A. & Forsythe, C. (2015)., Log analysis of cyber security training exercises. Proceedings of the Applied Human Factors and Ergonomics Conference, Las Vegas, NV.

[10] Stevens-Adams, S., Carbajal, A., Silva, A., Nauer, K., Anderson, B., Reed, T. & Forsythe, C. (2013). Enhanced training for cyber situational awareness, Proceedings of the Human-Computer Interactional International Conference, Las Vegas, NV.

[11] D'Amico, A., Whitley, K., Tesone, D., O'Brien, B., & Roth, E. (2005). Achieving cyber defense situational awareness: A cognitive task analysis of information assurance analysts. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting, SAGE Publications, 229-233.

[12] V.R. Kebande, I. Ray, A generic digital forensic investigation framework for internet of things (IoT), in: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Aug2016, pp.356–362.

[13] A.A. Cardenas, S. Amin, S. Sastry, Secure control: Towards survivable cyber physical systems, in: 2008 The 28th International Conference on Distributed Computing Systems Workshops, June2008, pp.495–500.

[14] E.A. Lee, Cyber physical systems: Design challenges, in: 2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC), May2008, pp.363–369.

[15] C.W. Tien, J.W. Liao, S.C. Chang, S.Y. Kuo, Memory forensics using virtual machine introspection for malware analysis, in: 2017 IEEE Conference on DependableandSecureComputing,Aug2017,pp.518–519.

[16] J. Gosling, B. Joy, G. Steele, G. Bracha, A. Buckley, The java virtual machine specification-javase8edition,feb.2015.

[17] G.Grispos, W.B.Glisson, K.K.R.Choo, Medical cyber-physical systems development: A forensics-driven approach, in: 2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE), July2017, pp.108–113.

[18] P. Bednar, A contextual integration of individual and organizational learning perspectives as part of IS analysis, Informing Science 3 (3) (2000) 145–156

[19] Washburn D, Sindhu U, Balaouras S, Dines RA, Hayes NM, Nelson LE. Helping IOS understand “smart city” initiatives: defining the smart city, its drivers, and the role of the CIO 2010; 12:2014. Retrieved April.

[20] Joe Haggerman, Michael Mylrea, Sri Nikhil Gupta Gourisetti, Andrew Nicholls, “Buildings Cyber security Framework”, PNNL-EERE Working Draft (Forthcoming) 2017