Analysis of Cybercrime Investigation Problems in the Cloud Environment

Grigor Khachatryan [1]
grigorkh@gmail.com
Director of Infrastructure Engineering Lyve Global LTD (https://lyveglobal.com/en), Abu Dhabi (Headquarters) 30th Floor, Capital Plaza Business Tower Abu Dhabi United Arab Emirates

Summary
Cloud computing has emerged to be the most effective headway for investigating crime especially cybercrime in this modern world. Even as we move towards an information technology-controlled world, it is important to note that when innovations are made, some negative implications also come with it, and an example of this is these criminal activities that involve technology, network devices, and networking that have emerged as a result of web improvements. These criminal activities are the ones that have been termed cybercrime. It is because of these increased criminal activities that organizations have come up with different strategies that they use to counter these crimes, and one of them is carrying out investigations using the cloud environment. A cloud environment has been defined as the use of web-based applications that are used for software installation and data stored in computers. This paper examines problems that are a result of cybercrime investigation in the cloud environment. Through analysis of the two components in play; cybercrime and cloud environment, we will be able to understand what are the problems that are encountered when carrying out investigations in cloud forensics. Through the use of secondary research, this paper found out that most problems are associated with technical and legal channels that are involved in carrying out these investigations. Investigator's mistakes when extracting pieces of evidence form the most crucial problems that take a lead when it comes to cybercrime investigation in the cloud environment. This paper not only flags out the challenges that are associated with cybercrime investigation in cloud environments but also offer recommendations and suggested solutions that can be used to counter the problems in question here. Through a proposed model to perform forensics investigations, this paper discusses new methodologies solutions, and developments for performing cybercrime investigations in the cloud environment.

Keywords:
Cloud computing, cybercrime, investigation challenges, digital evidence, cloud forensics.

1. Introduction

Among the technological productions that have been on the rise today as a result of improved information technology is that cloud computing. Cloud computing in this case defined as computer servers that can be accessed by the internet and databases and software that are responsible to run these servers, has emerged to be an important part of cybercrime investigations in forensics investigation [1]. The ability of cloud computing to place corporate data on the external server has proven to be effective in infrastructure building, security, and maintenance improvement for many consumers. Because of this, research has estimated a very steady increase of up to 160 billion dollars in expenditure as per the 2018 Cisco reports. This shows how important this part of cloud computing has become in these modern days.

The contribution of cloud computing and the cloud environment in general toward the solving of cybercrimes is overwhelming. Through a close analysis of the relationship between these two elements, one can develop an understanding that cybercrime investigation has been made possible through an improvement in the cloud computing system. Some of the major trends and problems associated with cloud computing in these modern days include the use of cloud environment as a business platform by criminals, using the cloud computing and cloud environment in general as an attacking tool like the DoS, and using the cloud as a platform for misuse of employees [2]. Because of this, the use of cloud computing platforms for cybercrime investigation forms an important source of forensic data that can be used to do investigations in case of cybercrimes.

However, in as much as this investigative platform seems effective for cybercrime investigation, research shows that many businesses and companies have not migrated to it due to the attached risks that come with it. This forms the thesis statement for this paper, such that through scientific and secondary research, we are going to explore different cybercrime investigation problems in cloud environments. Through answering the following research questions, we will be able to develop an understanding of these problems and possibly recommend possible solutions that can be used to solve these problems;

- Why should cybercrime investigation be done in the cloud environment?
- Can there be a possible solution for cybercrime investigation apart from the use of this cloud environment?

Manuscript received July 5, 2022
Manuscript revised July 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.7.38

- What are the challenges associated with the use of cloud environments in cybercrime and computer forensics?
- What are the solutions for some of the challenges that are associated with the use of cloud environments in cybercrime and computer forensics?
- What are possible recommendations for effective adaptable methodologies that can be used of obtaining electronic evidence that can be used in investigating cybercrime in a cloud-based environment?

By answering these research questions, this paper will meet the general goal and objective of the research which is a close analysis of the cybercrime investigation problems in the cloud-based environment.

This research incorporated the use of primary research through the use of interviews and questionnaires as a methodology procedure for obtaining data. Interviews here were focused on international law enforcement investigators that work at different forensic laboratories in the United States. In case the respondents were not ready for interviews, they had the option of filling in a questionnaire. Recommendations and solutions for problems were also added features that were additionally included in these methodologies, for effective attainment of this paper's objectives and goals.

2. Literature review

Previous research has given meaning to the two important terms that make up this paper, which is cloud environment and cybercrime. According to research, a cloud environment is obtained from computer computing, a very important element of forensics that forms crime investigation bodies.

Generally, cloud computing has been defined as a type of enabling ubiquitous model that enables convenient, and on-demand networking access to configurable computing resources which are used in management efforts through service provision and interaction [5]. Through cloud computing, research shows that this term has not been a new revelation but rather an available concept to marketers that have existed for decades. With its origin in the 1990s, cloud computing has led to increased web applications that have helped in the development of important applications such as Gmail and Facebook. Researchers have developed identifying key characteristics that make up this element of cloud computing. Some of them include the following; broad network access, on-demand self-service, measure service, rapid, scalability and elasticity, and resource pooling. These characteristics have made this software to be even more effective when it comes to cybercrime investigation.

Previous research shows that cloud computing has been divided into different models that it can be based on. These models include the private cloud model, a type of cloud computing that provides the infrastructure to a single customer [9]. The private cloud is usually owner-operated. The second cloud computing model is that of the community cloud. Her previous research shows that the community cloud provides infrastructure for a community with common interests that exclusively use it. The other model of cloud computing is that of the public cloud, a type of cloud computing that offers an infrastructure for use in the public sector, covering a wide range of users including the government, individuals, industry, or otherwise. The last model of cloud computing is the hybrid cloud which is simply a mixture of two or more models, which has the special feature of allowing data and applications to be shared in a compatible way.

To better understand the cloud environment, we have to understand first the functions of the cloud facility, either to the government or to individual companies [3]. These functions according to the study have been categorized into categories of software as a service is usually written as SaaS, platform as a service (PaaS), and infrastructure as a service appreciated as IaaS. The SaaS helps clients to contract providers to guide and manage the applications and infrastructure that businesses need to operate. Here, clients are allowed to direct different financial resources and time towards different income-generating portions [4]. The PaaS unlike SaaS allows clients to place into infrastructure created applications software with the help of languages, effective with the infrastructure. The last IaaS can offer clients an opportunity to manage the operating system, storage, and applications of the networking components of the infrastructure.

A close analysis of cybercrime from previous research shows that it has been one of the leading crimes in this modern era [8]. Cybercrime in this context is defined as any criminal activity that is carried out with the use of networking devices, networks, or computers in general. Usually, cybercrimes use this criminal activity to benefit themselves with profits while others do this to directly damage or disable important computers [10]. A person who for instance clears his disk to hide information in an office can be said to have committed a cybercrime. According to previous research, many different cybercrimes occur over the internet. These include crimes that occur targeting the computing device as a target, those that target computing devices as an instrument of crime, those that target computers as incidentals to a crime like that of money laundering, and those that target computers as a prevalence of software and hardware.

Many rising cases of cybercrime in the world today not only show advancement in the information technology sector but give us a reason to think that cybercrime happens for a reason. Previous research shows that

cybercrime is advantageous to criminals who seek to benefit from them, for instance, many of these crimes happen with intention of getting financial rewards [7]. However, this has not been limited to financial rewards only but also its proficient nature of happening without physical harm and effortless nature to commit. These crimes can be committed anywhere and it has been anticipated that as information technology improves so does these crimes increase with efficiency.

When we combine the two components of cybercrime and the cloud to give meaning to the main objective of this paper, we can say that cloud has offered an opportunity or rather a platform that has been effective in investigating cybercrimes. Research and recent forensics analysis show that in a cloud environment, cybercrimes occur there as a target for crimes and as a vehicle of facilitation that commissions different offenses. Many cybercrimes that occur in the cloud can be investigated, but research shows that they have been on the rise because of the attached problems that arise due to these investigation processes [4]. Example of crimes that occur on the cloud includes data intrusions, theft of intellectual property, and storage of dishonestly obtained data. Cloud platforms offer access to digital evidence that is used to carry out cybercrime investigations. Different models and functions of the cloud offer different effective platforms that can be sources of this digital evidence.

3. Methodology

This is a primary scientific research paper. Because of this, I employed the use of interviews and questionnaires to find the problems that most international experts in forensics encountered when investigating crime using the cloud environment. This being qualitative research, the interviews were offered directly to the respondents through online platforms such as Microsoft teams. Here, respondents were randomly chosen, a sampling technique that offered the opportunity to extensively interview a wide number of respondents for effective data collection. Through gaining different perspectives of this wide range of respondents, I was able to flag out the most commonly experienced problems that I sampled and included in the findings of this scientific research.

In two different forensic labs, I was able to find at least five respondents who were offered interview questions in order of their importance. The interview questions were designed in a way that allowed the respondents to give out general answers with no limitations, here, open-ended questions were used. When the interviews were over, respondents were allowed to give out a recommendation of the most effective strategies that they thought could be effective in dealing with the problems that they were facing in the forensics laboratories. Transcripts were therefore prepared for each interview and the electronic recordings that were obtained were closely examined. Some cases involved interviewees who did not want to be recorded, and therefore, only their transcripts were taken.

This research paper was not limited to only interviews but also questionnaires were involved. in a sample of five respondents that were taken from the labs, half of each were given questionnaires to fill. The questionnaires had both close-ended and opened-ended questions that were relevant to solving this scientific issue. Through the use of thematic analysis and quantitative analysis, a review of information obtained through interviews and the use of questionnaires was conducted. Organizations that were involved in this research study requested anonymity for respondents who offered to help carry out this research. This was a move to ensure that the respondents gave honest answers and comment that not only attributed to themselves but also to the organization in general. Only ten respondents were involved, 5 lawyers from the LEA agencies and 5 public prosecutors from forensic laboratories in the United States. Observations of the respondent's behaviors, the reflection of the conversations, and sharing of the information all contributed to this scientific research.

4. Results

Among the ten respondents that were interviewed, 9 of them gave relevant answers, and many of the answers given resembled each other, meaning that the problems were faced by both firms that were investigated for this study. The results obtained were as follows

Table 1: Challenges facing cybercrime investigation in the cloud environment

Challenges	Suggested solutions	Analysis comments
The first problem that was identified as the problem of decentralized data, a problem that was flagged by 80% of the respondents.	Log framework was proposed as a solution to this problem.	Here, log frames were seen to be effective in dealing with this issue of decentralized data. Log frameworks allow data to be effectively created, processed, stored, and distributed to different data centers through the use of physical machines. Here stored data is replicated fragmented and distributed.
The problem of dependence on CSP	SLA specification of forensic service.	Through the use of effective SLA specification of forensic services, research shows that effective accessibility

		and consistency benefits are achieved, overcoming greatly the problem of dependence on CSP.
Unknown physical location problems.	Tagging of resources, robust SLA with CSPs, and using the SLA with cloud forensics form the perfect solution to this cybercrime problem usually experienced in the cloud environment.	CSPs are effective means used in forensic labs to ensure the flexibility and manageability of services offered. Through this, SLA guidelines substitute it, containing guidelines that should be followed in forensics, hence avoiding these problems that are associated with unknown location problems.
The problem of deleted data.	Taking snapshots frequently.	When carrying out cybercrime investigations in forensic laboratories, more often investigators find it difficult to retrieve important information that is used to supplement investigations because it was deleted. Because of this, using media data carving can help retrieve deleted data; however, a more effective move here is the use of snapshot images.
The problem of data volatility	Training of forensics live trainees can help reduce such problems.	The complex nature of forensics data collection is complemented by training and support from outside sources. And because of this, popular isolation methods of vendors from genuine users are achieved.
The problem of very complex cloud	The lining of events timely	This makes it difficult to explain the complex nature of the cloud, making it possible for vendors to outshine security measures, hence creating room for criminal activities. The effective lining of events in forensic laboratories helps eradicate such problems.
Encrypted data	Management of cloud key infrastructure	This makes it effective to possibly implement plans to eradicate the problem of encrypted data.

Through a close analysis of data obtained, it is clear that the problems of decentralized data, deleted data, and data integrity are the ones facing the cybercrime investigation process in the cloud environment. Through this, possible solutions and recommendations were examined and effectively incorporated as shown in the table above.

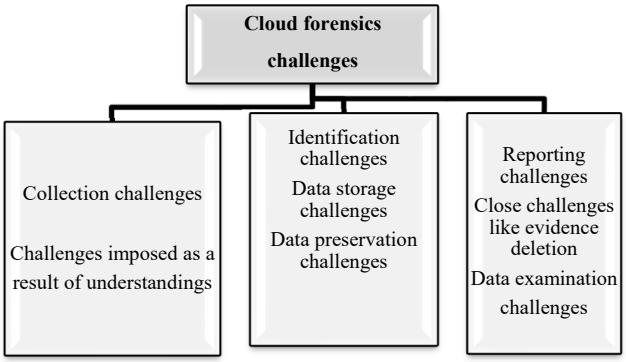

Fig.1. Cloud forensics challenges

5. Recommendations

Carrying out cybercrime investigations in the cloud cannot be that easy unless a better solution is achieved that can eradicate most of the problems that are faced when carrying out this exercise. Because of this, a model that can perform investigations in forensics in a cloud environment using digital data forms a perfect recommendation that can be adapted to deal with this situation. The model here is termed the model of digital forensics processes in a cloud environment that dictates that activities should be distinguished when clients of play make any movements in the cloud environment [6]. Transferring malware to different platforms and limiting the number of downloads are some of the strategies that this model proposes. The use of an Intrusion detection system forms one of the most recent developments proposed by this model that can be used to consolidate all virtual machines used in organizations. This feature not only protects machines from external invasion but also notifies users of possible malicious activities that are a result of cybercrime.

5. Conclusion

Cybercrimes are on the rise and companies and individuals are losing lots of money to cybercriminals. Because of this, forensic laboratories have been allowed to bring an end to these malicious activities but this paper has indicated that this is not possible because there are so many problems that have been attached to this. Cybercrime investigation is becoming a limitation and the answer to this problem cannot be found unless proposed developments have been made to ensure safety in offices and even in our homes. The government must shift its focus from normal criminals to cyber criminals because they are exploiting and affecting many businesses in the world as compared to the commonly known criminals. Encouraging forensic investigations through a close examination of the problems that they encounter can help greatly deal with this situation. Provision of resources and improvement of the information technology system in our offices forms a dependable move that can help resolve most of the problems facing cybercrime investigations in the cloud environment.

References

[1] R. Anderson *et al.*, *Measuring the Changing Cost of Cybercrime*. 2019 *The 18th Annual Workshop on the Economics of Information Security* https://doi.org/10.17863/CAM.41598

[2] A. Abbasi, A. Abbasi, S. Shamshirband, A. T. Chronopoulos, V. Persico, and A. Pescape, "Software-Defined Cloud Computing: A Systematic Review on Latest Trends and Developments," *IEEE Access*, vol. 7, pp. 93294–93314, 2019. Accessed: Jun. 17, 2022. [Online]. Available: https://doi.org/10.1109/access.2019.2927822

[3] M. Adhikari, T. Amgoth, and S. N. Srirama, "A Survey on Scheduling Strategies for Workflows in Cloud Environment and Emerging Trends," *ACM Computing Surveys*, vol. 52, no. 4, pp. 1–36, Sep. 2019. Accessed: Jun. 17, 2022. [Online]. Available: https://doi.org/10.1145/3325097

[4] M. Y. Arafat, B. Mondal, and S. Rani, "Technical Challenges of Cloud Forensics and Suggested Solutions," *International Journal of Scientific & Engineering Research*, vol. 8, no. 8, pp. 1142–1149, Aug. 2017. Accessed: Jun. 17, 2022. [Online]. Available: https://doi.org/10.14299/ijser.2017.08.004

[5] Eivy and J. Weinman, "Be Wary of the Economics of "Serverless" Cloud Computing," *IEEE Cloud Computing*, vol. 4, no. 2, pp. 6–12, Mar. 2017. Accessed: Jun. 17, 2022. [Online]. Available: https://doi.org/10.1109/mcc.2017.32

[6] Knauer, "How contact centres can leave businesses exposed to cybercrime," *Network Security*, vol. 2019, no. 11, pp. 6–9, Nov. 2019. Accessed: Jun. 17, 2022. [Online]. Available: https://doi.org/10.1016/s1353-4858(19)30130-8

[7] E. E.-D. Hemdan and D. H. Manjaiah, "Digital Forensic Approach for Investigation of Cybercrimes in Private Cloud Environment," in *Advances in Intelligent Systems and Computing*. Singapore: Springer Singapore, 2018, pp. 25–33. Accessed: Jun. 17, 2022. [Online]. Available: https://doi.org/10.1007/978-981-10-8639-7_3

[8] J. Kremling and A. M. S. Parker, *Cyberspace, Cybersecurity, and Cybercrime*. SAGE Publications, Inc, 2017.

[9] H. S. Lallie *et al.*, "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Computers & Security*, vol. 105, p. 102248, Jun. 2021. Accessed: Jun. 17, 2022. [Online]. Available: https://doi.org/10.1016/j.cose.2021.102248

[10] K. M. Rajasekharaiah, C. S. Dule, and E. Sudarshan, "Cyber Security Challenges and its Emerging Trends on Latest Technologies," *IOP Conference Series: Materials Science and Engineering*, vol. 981, p. 022062, Dec. 2020. Accessed: Jun. 17, 2022. [Online]. Available: https://doi.org/10.1088/1757-899x/981/2/022062

Grigor Khachatryan (Գրիգոր Խաչատրյան), Director of Infrastructure Engineering Lyve Global LTD (https://lyveglobal.com/en), Abu Dhabi (Headquarters) 30th Floor, Capital Plaza Business Tower Abu Dhabi United Arab Emirates, ORCID: 0000-0002-6735-7149