

**A PLATFORM FOR DIGITAL CRIME SCENE  
RECONSTRUCTION ON A CLOUD COMPUTING  
ENVIRONMENT**

BY

**KEEMBIYE HETTIGE AKALANKA HETTIGE**

A thesis submitted to the **Faculty of Applied Sciences, Rajarata University of Sri Lanka**  
in partial fulfillment of the requirements for award of the degree of  
**MASTER OF PHILOSOPHY in COMPUTER SCIENCE**

Faculty of Applied Sciences  
Rajarata University of Sri Lanka  
Mihintale – Sri Lanka  
November 2022

ACC NO.	PGT 0004
CALL NO.	005 - 447HET

## **ABSTRACT**

Cloud computing is an emerging area in computing. The idea of cloud computing is to have a server farm where the clients are allowed to rent computing resources such as Virtual Machines, processing power, and storage space through the Internet. Cloud forensics is the branch of computer forensics that is dedicated to crime scene investigations on cloud computing platforms. Given the nature of cloud computing platforms, usual forensics methods face issues when being used on them. This research aimed to develop a forensics platform to be used on cloud computing platforms. Cloud infrastructure is owned by a service provider, the client does not get access to the hardware even during a security incident. Of the cloud computing models, the one which gives the most privileges to the client is known as Infrastructure-as-a-Service or IaaS. Therefore, the research focused on IaaS cloud platforms. Considering IaaS platforms, 76% of the market is dominated by four Cloud Service Providers (CSP). Comparing the forensic support provided by each CSP, they are a significant disparity. However, given the technical details of each CSP, it seems that all of the support functions can be used during a forensic investigation. According to the literature, one of the pressing issues that are facing cloud forensics is the issue of time taken for an investigation. In the absence of enough empirical evidence for this fact, several experiments were conducted to measure the performance of the Autopsy forensic tool over increasing loads of source data. The experiments showed that full analysis of a forensic image becomes impractical when the evidence sources go into Tera or Peta Byte ranges as it is common on cloud platforms. Therefore, some form of prioritizing of evidence is required. Another pressing issue is the trustworthiness of the CSP. A set of algorithms was proposed to ensure the trustworthiness of the evidence by checking for integrity. To combine both of these issues, a comparison between the forensic evidence sources in a cloud, a standalone web server, and a standalone computer showed that cloud platforms contain additional log files provided by the CSP. Focusing on the log files, algorithms were created to parse through log files and categorize them according to the timestamps and IP address. During experimentation, the algorithms showed results within five minutes for log files large as 4.9GBs while correctly identifying the timestamps. On the other hand, Autopsy took 33 minutes for the analysis without identifying any timestamp in the content of the log files. Further graphical analysis of the results shows that outlier entries stand out.

## Contents

CHAPTER 1 .....	1
RISE OF CLOUD COMPUTING AND THE PHENOMENON OF CYBERCRIME.....	1
1.1 Introduction.....	1
1.1.2 Computer Crimes and Digital Forensics .....	3
1.1.3 Criminal potential in the cloud .....	6
1.2 Digital Crime Scene Reconstruction on a Cloud Computing environment .....	8
1.3 Research inspiration .....	11
1.4 Analysis of the research problem .....	12
1.4.1 Problem statement .....	12
1.5 Research objectives and questions .....	13
1.5.1 Research objectives .....	13
1.5.2 Research questions .....	13
1.6 Research methodology .....	14
1.7 Thesis outline .....	15
CHAPTER 2 .....	16
EXPLORATION OF BACKGROUND AND ISSUES OF CLOUD FORENSICS.....	16
2.1 Introduction.....	16
2.2 Background of Cloud Computing.....	16
2.3 Digital Forensics .....	21
2.3.1 Digital Forensic Process Models .....	22
2.4 Issues in cloud forensics.....	32
2.4.1 Selected publications that discuss issues in cloud forensics.....	33
2.4.2 Conclusions from the selected publications .....	42
2.5 Cloud forensic process models.....	44
2.5.1 Selected models .....	44
2.5.2 Conclusions from the selected cloud forensic models.....	50
2.6 Conclusions .....	51
CHAPTER 3 .....	52
IMPLEMENTATION AND TESTING .....	52
3.1 Introduction .....	52
3.2 Testing of existing tools .....	52

3.2.1 Experiment 1.....	53
3.2.2 Experiment 2.....	54
3.2.3 Experiment 3.....	54
3.2.4 Experiment 4.....	55
3.3 Cloud model.....	55
3.3.1 Requirements of the cloud model.....	55
3.3.2 Comparison of major service providers.....	59
3.4 The model.....	63
3.4.1 The initial decision: dead or live .....	65
3.4.2 Trustworthiness through integrity .....	66
3.4.3 Speeding up the process .....	71
3.5 Implementation.....	75
3.5.1 Integrity checking on logs .....	75
3.5.2 Integrity checking on JSON .....	78
3.6 Experimentation on our program .....	79
3.6.1 Experiment 5.....	79
3.6.2 Experiment 6.....	81
3.6.3 Discussion of the experimental results .....	82
3.7 Summary .....	84
CHAPTER 4 .....	85
CONCLUSIONS AND FUTURE WORK .....	85
4.1 Introduction .....	85
4.2 Research findings .....	85
4.2.1 Achievement of research objectives .....	86
4.2.2 Answers to the research questions .....	87
4.3 Conclusions .....	88
4.4 Limitations and Future directions .....	88
References .....	90
APPENDICES .....	i
Appendix A.....	i
PUBLICATIONS.....	xxii