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

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