Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 110 (2017) 336–343

Procedia Computer Science

www.elsevier.com/locate/procedia

The 12th International Conference on Future Networks and Communications (FNC-2017)

Secure Logging as a Service Using Reversible Watermarking

Abid Khan*, Ayyaz Yaqoob, Kinza Sarwar, Mouzna Tahir, Mansoor Ahmed

Department of Computer Science, COMSATS Institute of Information Technology, Park Road Chak Shahzad, Islamabad, Pakistan

Abstract

Logs are very important as they provide details of a systems past events as well as help in system monitoring, troubleshooting and forensics. In order to be useful the logging process must be done in a secure manner and logging files must be kept secure for an extended period of time as they may contain sensitive information. However, deploying a logging infrastructure is an expensive and time-consuming task. A natural solution to this problem these days is to use cloud storage for keeping logs, because of the benefits provided by cloud computing thus delegating the log management to a cloud service provider (CSP). This paper introduces secure log as a service using reversible watermarking (SecLaaS-RW) scheme. Reversible watermarking is a type of fragile watermarking, which can be used for content authentication. The content in our case are outsourced logs, to which reversible watermarking is applied. Log records are collected using syslog, processed at the logging server and then transferred to an outsource cloud storage, where all records are saved for extended period of time. We have made comparison with a recently proposed scheme. Our experimental results suggest that with a very limited and manageable overhead per log entry, modifications in the outsourced logs can be detected.

Keywords: *secure logging;forward secrecy; cloud computing; reversible watermarking*

1. Introduction

Cloud Computing has provided the next evolutionary step of IT services deployment and their delivery mechanism. Virtualization is used as the enabling technology to achieve on demand delivery of services, reliability, multi-tenancy, scalability and elasticity [1]. The deployment models used by cloud computing are private cloud (internal datacenters of business or organizations which are not available for general public use)[2], public cloud (private cloud made accessible for general public use on pay-as-you-go model) hybrid/multi cloud. The services in cloud computing environment are organized as IaaS, PaaS, and SaaS. Under the umbrella of these services, many new kinds of services have emerged[3,4,5]. Logs are used extensively to monitor and record the current and past state of a computer system. This makes logging the most fundamental digital forensic method to provide security and reliability in modern distributed computing systems. Traditionally a logging mechanism is deployed in order to record the malicious activities. This

* Corresponding author. Tel.: +92-051-9049-5330 ; fax: +0-000-000-0000.
E-mail address: abidkhan@comsats.edu.pk

10.1016/j.procs.2017.06.103

may include software working, data access or modifications and user activities. Logging is essential, because it can be used to achieve some important tasks such as troubleshoot software, handle system performance issues etc[6,7]. Since, audit logs are an important aspect of forensics, therefore an experienced attacker would target them. The attacker may try to remove the traces of his presence and malicious activities performed by him. There are several applications, which can benefit from a secure audit logs such as an intrusion detection system (IDS), mobile computing agents, and a computer under the control of a marginally trusted entity. Due to extensive adoption of network infrastructure and the ever increasing number of internal and external threats against networks, the need of having a secure logging mechanism have amplified tremendously. It is important to have secure and correct versions of audit logs. Any tampering in the logs must be detectable. However, achieving this might not be so easy, specially todays distributed systems such as cloud computing or smart grids. It is extremely challenging to provide confidentiality and integrity of the outsourced data[8], because it is difficult to detect unauthorized modification or tampering with the data. However, logs data must be protected from tampering in order to enable the detection and the investigation of security violations. Such system is required that keep log record of the system secure. Therefore, in this paper, we propose a system to ensure the privacy; security, modification and reliability of log batches over the cloud-based infrastructure, such that these logs are verifiable by trusted third party. To illustrate the problem practically, consider the following scenario:

Suppose Alice is a successful business merchant who hosts a website on the cloud infrastructure. Alice is selling products and also providing various other services. Her business runs successfully and she cannot afford to be offline even for an hour. Bob, who is the Cloud Service provider (CSP) manages all the logs for that website. Eve having malicious intentions have also rented some machines on the same cloud infrastructure to perform a denial of service attack on Alices website. As a result, Alices website remains unavailable for more than an hour. Now, Alice asks a trusted third party (TTP) to investigate the case of why her website was unavailable for such a prolonged time.

In above scenario Alices website logs are recorded and store on cloud. The trusted third party accesses those logs on cloud and investigates the matter. Digital Watermarking embeds a secret in a digital content with the help of a key[9]. Only the person in possession of this key can retrieve the original content. Reversible watermarking is a special kind of watermarking technique, in which we can retrieve “original un-watermark content”, when the watermark content is authenticated [10,11]. To achieve confidentiality, we have used reversible watermarking and access control mechanism. Reversible watermarking is implemented, which will provide strong guarantees of logs integrity and tamper-proofing. Furthermore, any modification in logs will be detectable in watermark extraction phase. For encryption and integrity secure hash algorithm is implemented. The proposed system will be beneficial in case of system crash or in troubleshooting. The user can view logs from log as a service and solve and can keep track of various activities performed by a user in an organization. Real-world applications of secure logging includes:

- Data forensics: Secure logging scheme ensures that the data required for correlation, forensic investigation and reporting has been originated and fetched correctly. It enables the log consumers to efficiently analyse, correlate and process the emitted log files. In this context, it provides the oriented logging framework platform for log analysts and service owners to understand the status of fault and performance monitoring, incident detection, standard compliance, business processes and access logs historic information.
- Audit trial: Secure logging schemes presents auditing features to enable the end-users and system administrators to audit log data file access, changes and allocation, transfer and life cycle histories. Moreover, secure logging schemes have supported the automated audit logs of an encrypted data compliance with the user-defined security policies.
- Performance tuning: Secure logging techniques have achieved audit logs scalability through optimizing the performance of production and consumption processes.
- Troubleshoot problems: Secure logging schemes have allowed log analyst or end-users to troubleshoot errors occurred during transmission, log files access, retrievability and transfer problems such as system administrators, which used security log tools to troubleshoot problems.
- E-Commerce: One of the rich applications of secure logging is in e-commerce based environment, where secure logging techniques are used to achieve a variety of security services.
- Healthcare web applications: Mobile healthcare systems have integrated different logging schemes with the web applications to protect entire identity management system and to prevent security attacks.