Chapter 13
Development of Secured Log Management System Over Blockchain Technology

Sagar Shankar Rajebhosale
SF's SITRC, Nashik, India

Mohan Chandrabhan Nikam
SF's SITRC, Nashik, India

ABSTRACT

A log is a record of events that happens within an organization containing systems and networks. These logs are very important for any organization, because a log file will able to record all user activities. Due to this, log files play a vital role and contain sensitive information, and therefore security should be a high priority. It is very important to the proper functioning of any organization, to securely maintain log records over an extended period of time. So, management and maintenance of logs is a very difficult task. However, deploying such a system for high security and privacy of log records may be overhead for an organization and require additional costs. Many techniques have been designed for security of log records. The alternative solution for maintaining log records is using Blockchain technology. A blockchain will provide security of the log files. Log files over a Blockchain environment leads to challenges with a decentralized storage of log files. This article proposes a secured log management over Blockchain and the use of cryptographic algorithms for dealing the issues to access a data storage. This proposed technology may be one complete solution to the secure log management problem.

INTRODUCTION

A log file is the record of detailed information of each and every event of a system, network or application running in an organization (Indrajit Strizhov, Mulamba, and Rajaram, 2013). When different operational issues occur in a system, Log file provides useful knowledge to resolve those issues. To distinguish policy violations, illegal activities and protection incidents the log files are extremely helpful. Because

DOI: 10.4018/978-1-7998-5351-0.ch013

logs contain very sensitive information about every activity, it is important to have extra protection from malicious attackers for log files. Since log files contain record of most system events as user activities, malicious attackers may choose those files as a significant target for attack on the organization (Ma & Tsudik, 2009). Associate attacker typically would try to not leave evidence or traces of his or her activities behind as they were breaking into a system.

GENERATION OF LOG FILES

To generating logs several protocols are supported syslog (Kent & Murugiah, 2006), Syslog-ng (Lonvick, 2001), Reliable delivery of syslog (New & Rose, 2001), syslog-pseudo (Fleugel, 2002), forward integrity for audit logs (Bellare & Yee, 1997), and syslog-sign (Kelsey, Callas, and Clemm, 2010) are some security extensions projected to syslog. They were not able to firmly secure the log files as they provide partial protection, or no protection of the log records from malicious attacks. On different side the format, size and count of security logs have increased rapidly. That needs of some extra features to log management like different techniques for generating, transmitting, storing, analyzing, and eliminating security log data (Indrajit Strizhov, Mulamba, and Rajaram, 2013).

MAINTENANCE OF LOG FILES

Organizations facing serious issues with log management. For any organization, maintenance of log are typically difficult for several reasons, additionally a high range of log sources; inconsistent log formats, content and timestamps among sources; and huge volumes of log information (Ma & Tsudik, 2009). Log management additionally must consider some properties like confidentiality, integrity, and availability of logs. For deploying secure work information to meet all the above challenges, cloud storage seems to be the best option.

WHY BLOCKCHAIN?

Blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptographic algorithms (Peck, 2017). Blockchain is an open, distributed, public ledger that can record transactions between two parties efficiently and in a verifiable and permanent way (Gopal, 2016). Presently, the emerging Blockchain paradigm is rapidly gaining momentum as an alternative to traditional information technology. Blockchain technology is like the internet in that it has a built-in robustness.

By storing blocks of information that are identical across its network, the Blockchain cannot:

1. Be controlled by any single entity
2. Has no single point of failure (Peck, 2017)

It provides a scalability environment for growing amounts of data and processes that work on various applications and services by means of on demand self-services. One fundamental aspect of this paradigm shift is that data are being decentralized and outsourced into nodes (blocks). This kind of outsourced