Chapter 28
Monitor and Detect Suspicious Transactions With Database Forensic Analysis

Harmeet Kaur Khanuja
MMCOE, SPPU, Maharashtra, India

Dattatraya Adane
Shri Ramdeobaba College of Engineering and Management, Nagpur, India

ABSTRACT

The extensive usage of web has given rise to financially motivated illegal covert online transactions. So the digital investigators have approached databases for investigating undetected illegal transactions. The authors here have designed and developed a methodology to find the illegal financial transactions through the database logs. The objective is to monitor database transactions for detecting and reporting risk level of suspicious transactions. Initially, the process extracts SQL transactions from logs of different database systems, then transforms and loads them separately in uniform XML format which gives the transaction records and its metadata. The transaction records are processed with well-defined rules to get outliers present as suspicious transactions. This gives the initial belief of the transactions to be suspicious. The belief value of transactions is further rationalised using Dempster-Shafer's theory. This verifies the uncertainty and risk level of the suspected transactions to assure occurrences of fraud transactions.

INTRODUCTION

The technological advancement and the globalization of online banking provisions for finance and the payment systems have widened the scope of concealing illegal money and easy mobility of funds across the borders. These are known as suspicious activities or illegal transactions incorporating money laundering. Theodosios Tsiakis et al. (2015) recommend the need to manage and regulate the risks calls for Information Technology Security Governance (ITSG) program as a means to deliver value business

DOI: 10.4018/978-1-7998-3025-2.ch028

and mitigate Information Technology (IT) risks. Their objectives are to implement information security governance (ISG) approaches for e-banking through standards, guidelines on governance, risk management methods and internal controls for e-banking. Streff (2007) outlines the importance of IT security to banks which must comply with law and regulation of banks. D. Rafal et al. (2012) mentioned an illegal transaction of money is now a global problem which can undermine the integrity and stability of financial markets and financial institutions (FI). As per Reserve Bank of India (RBI, 2017), the Banks and FIs should exercise ongoing due diligence with respect to every customer and closely examine the transactions to ensure that they are consistent with the customer's profile and source of funds as per extant instructions. Palshikar et al. (2014) suggests that prevention, detection and control of money laundering are crucial for the financial security and risk management of financial institutions. Conversely, Anti-Money Laundering (AML, 2015) Transaction Monitoring systems produce large volumes of work items most of which do not result in quality investigations or actionable results.

To avert this government act like Sarbanes-Oxley (SOX, 2017) has given an immense impact on database auditing requirements. Patnaik et al. (2003) mentions that the survivability of database systems in case of information attacks depends exclusively on the logging mechanism. This process requires that the log must record all operations of every transaction and that the log should never be purge, but these results in enormous growth of the logs. They used logs based on transaction relationships and stored each segment as a separate file to access independently as required. As suggested by H. Khanuja et al. (2014), S. Raghavan (2013), H. Beyers et al. (2011), M. Olivier et al. (2012), database audit logs contain traces of information which can be used for investigations. These audit logs if administered and carefully monitored to record database activities, can contour suspicious and illegal behaviour acts. Thus, the monitoring systems and log collection must provide an audit trail of all the activities and access to sensitive business information.

To deal with this problem this research aims to pioneer database forensics by probing database systems and their native database audit logs for monitoring and reinstate evidences. Database forensics is a subset of application-based forensics, which identifies, preserves and analyses digital information within databases to produce evidence in a court of law. F. Kevvie (2009) said examining database artifacts is the most relevant to database investigations. The information obtained through it can be collected and preserved very safely and non-disruptively to analyze and confirm database intrusions. This also facilitates an investigator to retrace the actions of an intruder within a database server. According to D. Litchfield (2007), SQL operations leave plenty of forensic data onto database infrastructure in the Oracle server for forensic analysis. Thus, this article presents a very thorough discussion of a framework which uses database audit logs for detecting suspicious transactions in a financial scenario. Since the database systems have their own database auditing capabilities so two databases viz; Oracle and MS SQL databases were experimented for this research work.

RELATED WORK

Various approaches are studied and surveyed to detect suspicious transactions. It is discussed in the paper P. Kanhere et al. (2014) and H. Jiawei et al. (2012) that the outliers in database transactions, translated into significant information can be useful for analysis and activity reporting. H. Kuna et al. (2014) suggests that auditors can use data mining techniques to analyse the data and identify outliers. They designed and developed a methodology to assist the auditor in anomalous data detection within