Chapter 12
To Monitor and Detect Suspicious Transactions in a Financial Transaction System Through Database Forensic Audit and Rule-Based Outlier Detection Model

Harmeet Kaur Khanuja
Marathwada Mitra Mandal's College of Engineering, India

Dattatraya Adane
Shri Ramdeobaba College of Engineering and Management, India

ABSTRACT

The objective of this chapter is to monitor database transactions and provide information accountability to databases. It provides a methodology to retrieve and standardize different audit logs in a uniform XML format which are extracted from different databases. The financial transactions obtained through audit logs are then analyzed with database forensic audit. The transactions are examined, detected, and classified as per regulations and well-defined RBI antimony laundering rules to obtain outliers and suspicious transactions within audit logs. Bayesian network is used in this research to represent rule-based outlier detection model which identifies the risk level of the suspicious transactions.

INTRODUCTION

As per, FICCI- Federation of Indian Chambers of Commerce and Industry – Pinkerton India Risk Survey 2017, 'Information & Cyber Insecurity' has become more distinct due to the change that the nation which is undergoing towards digitization of various assets. It is said in the FICCI release, that the recent demonetization saw a spike in the number of people resorting to online platforms for financial transac-

DOI: 10.4018/978-1-5225-7356-2.ch012

tions. This is posturing greater risks for users, including businesses, e-commerce etc. Also there is tremendous increase in subscribers to the Unique Identification Number (UIN) where personal information is stored as data which are linked to the banking details. The businesses are legally required to retain certain types of information and data in their databases for various periods of time as per requirements in every state and country; hence it becomes critical to stop deleting any form of electronic records that might be related to the case. This is giving opportunities to hackers to commit a breach. This may also lead to increase in existing risks in the cyber domain, such as money laundering and identity theft.

In developing countries, the security is becoming complicated with rapid expansion of access to the Internet, an unprecedented understanding of technology, increasing economic competition, and the push to achieve greater efficiencies. 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. In financial transactions, people hide their actions through a series of steps that make it look like money coming from illegal or unethical sources which was earned legitimately. Financial institutions are required to keep an eye on database transactions to detect the abnormality or any suspicious activity carried out if any. This will prevent such cases and submit the detailed reports to the regulatory bodies.

Indeed, in today's business world, almost all applications use databases to manage data. Here the focus is on databases of banking transactions. Fraudulent banking activities are becoming more and more sophisticated which is threatening the security and trust of online banking business resulting as a major issue for handling financial crimes. It is now a global problem which can undermine the integrity and stability of financial markets and financial institutions. Moreover it is becoming challenging due to the Money Laundering practices carried over.

In view of this, the government act like Sarbanes-Oxley Audit Requirements (SOX) ("Sarbanes Oxley Audit Requirements", 2018) has an immense impact on database auditing requirements. Consequently, the monitoring systems and log collection must provide an audit trail of all the activities and access to sensitive business information. As per Reserve Bank of India (RBI) ("Master Direction - Know Your Customer (KYC) Direction", (2016)), the Banks and Financial institutions should exercise ongoing due diligence concerning every customer and carefully examine the transactions to ensure that they are consistent with the customer's profile and source of funds as per extant instructions. The Regulations of Reserve Bank of India for Anti-money Laundering (AML) defines the standard rules for suspecting the illegal transactions. The AML systems produce large volumes of work items, but very few results in quality investigations or actionable results. Effective and efficient detection of Anti Money Laundering is regarded as a major challenge to all the banks and is an increasing cause for concern. One way to ensure this is to keep end-to-end accountability of databases through continuous assurance technology and transaction monitoring with Digital forensics. This has motivated us to develop a methodology which monitors the database transactions and retain evidences to prove the transactions to be legitimate or suspicious. The suspicious transactions can then be used for investigations to reconstruct the illegal activity carried out in an organization. This can be achieved by incorporating information accountability in Database Management System.

This chapter presents a comprehensive discussion of a proposed methodology to detect suspicious transactions through forensic audit in a financial scenario which considers standard RBI rules implemented for countering frauds such as money laundering. The information retrieved through database audit logs is used to analyze hidden values. The suspected transactions are verified using Dempster-Shafer's