WEB-BASED INTERFACE FOR CONTROL OF BANK STAFF FRAUD

T. O. Oladele
Department of Computer Science
University of Ilorin
Ilorin, Kwara State, Nigeria
tinuoladele@gmail.com, oladele.to@unilorin.edu.ng
+234 8164916082,

O. A. Fadipe-Joseph
Department of Mathematics
Ilorin, Kwara State, Nigeria
famelov@unilorin.edu.ng
+234 8033972496

ABSTRACT
Fraud is a big business deal and it is increasing every year. Fraud involves one or more persons who intentionally act in secret in order to deprive another of something of value for their own gain and benefit. Fraud is as old as humanity and it can take uncountable number of forms. Bank fraud is not new in the Nigerian Banking Industry but the rate at which bank staff are involved in bank fraud calls for serious attention and intervention. A lot of individuals and organizations yearly lose resources worth billions of naira to bank fraud which are perpetrated by bank staff. Hence, urgent measures should be taken to curb and control the involvement of bank staff in fraudulent acts. In this paper, we carried out a computational method of controlling bank staff fraud by using a data mining technique which is based on ledger assessment and job rotation. The technique of controlling bank staff fraud introduced in this work cannot be influenced by the bank management and the bank staff cannot predetermine when his ledger would be assessed or when his job would be rotated. The Fraud control system provides a web-based interface that was designed using PHP as a scripting language, with MYSQL relational database on Apache server under Windows 7 operating system platform and using CSS (Cascading Style Sheet) and HTML.

Keywords: Fraud, Embezzlement, Bank, Job Rotation.

1. INTRODUCTION
Fraud is an act which is intended to cause unlawful gain to one person and wrongful loss to the other, either by way of concealment of facts or otherwise. Fraud can be seen as the intentional misrepresentation, concealment or omission of the truth for the purpose of deception, manipulation to the financial detriment of an individual or an organization (such as a bank) which also includes embezzlement, theft or any attempt to steal or unlawfully obtain, misuse or harm the asset of the bank. (Adeduro A. A., 1998, and Bostley R. W. B. and Drover C. B., 1972). Fraud has been the major factor in the distress of banks. Despite various measures that have been taken to minimize the incidence of fraud, it still rises by the day because fraudsters always devise new, sophisticated and tactical ways of committing fraud. This has become an issue of great concern in the banking sector as well as many organizations in Nigeria. Fraud has a long term effect of reducing the assets and thereby increasing the liability of any company. In the case of banks, this may result in the loss of potential customers or crisis and in the long run end up in another failed bank situation (Abiola I., 2009).

Fraud is one of the numerous enemies of the business world. No company or organization is immune to it. It occurs in all works of life, in government, the export trade, shipping transactions, banking, insurance and everywhere. Special organizations have been formed to prevent it and the international police (Interpol) tries to deal with it at the international level, but it has not and cannot be eradicated (Nwankwo G. O., 1991). Fraud is a universal phenomenon which has been in existence for a long time. However, in recent years, the development of new technologies has also provided further ways in which criminals may commit fraud (Bolton R. and Hand D., 2002). In addition, business re-engineering, re-organization or downsizing may weaken or eliminate control, while new information systems may provide additional opportunities to commit fraud. It is pertinent to note that no area of the banking system is immune to fraudsters, not even the security team designated to prevent it. Hence, the prevention and control of bank staff fraud has become a herculean task which requires serious and urgent intervention. Fadipe-Joseph et al (2012) established the application of continued fraction in controlling bank fraud. In this paper, we have adopted the ledger assessment and rotation technique in the control of bank staff fraud.
2. DATA ANALYSIS TECHNIQUES FOR FRAUD DETECTION

Various data analysis techniques have been adopted in the past for fraud detection in different organizations and business firms.

2.1 Detecting Fraud

Traditional ways of data analysis have been in use since long time as a method of detecting fraud. They require complex and time-consuming investigations that deal with different domains of knowledge like financial, economics, business practices and law. Fraud often consists of many instances or incidents involving repeated transgressions using the same method. Fraud instances can be similar in content and appearance but usually are not identical (Palshikar G. K., 2002). Fraud that involves cell phones, insurance claims, tax return claims, credit card transactions etc represent significant problems for governments and businesses, but yet detecting and preventing fraud is not a simple task. Fraud is an adaptive crime, so it needs special methods of intelligent data analysis to detect and prevent it. These methods exist in the areas of Knowledge Discovery in Databases (KDD), Data Mining, Machine Learning and Statistics. They offer applicable and successful solutions in different areas of fraud crimes.

Techniques used for fraud detection fall into two primary classes: statistical techniques and artificial intelligence (Palshikar G. K., 2002). Examples of statistical data analysis techniques are:

- Data preprocessing techniques for detection, validation, error correction, and filling up of missing or incorrect data.
- Calculation of various statistical parameters such as averages, quartiles, performance metrics, probability distributions, and so on. For example, the averages may include average length of call, average number of calls per month and average delays in bill payment.
- Models and probability distributions of various business activities either in terms of various parameters or probability distributions.
- Computing user profiles.
- Time-series analysis of time-dependent data.
- Clustering and classification to find patterns and associations among groups of data.
- Matching algorithms to detect anomalies in the behavior of transactions or users as compared to previously known models and profiles. Techniques are also needed to eliminate false alarms, estimate risks, and predict future of current transactions or users.

Fraud management is a knowledge-intensive activity. The main AI techniques used for fraud management include:

- Data mining to classify, cluster, and segment the data and automatically find associations and rules in the data that may signify interesting patterns, including those related to fraud.
- Expert systems to encode expertise for detecting fraud in the form of rules.
- Pattern recognition to detect approximate classes, clusters, or patterns of suspicious behavior either automatically (unsupervised) or to match given inputs.
- Machine learning techniques to automatically identify characteristics of fraud.
- Neural networks that can learn suspicious patterns from samples and used later to detect them.

Other techniques such as link analysis, Bayesian networks, decision theory, and sequence matching are also used for fraud detection (Palshikar G. K., 2002).

2.2 Machine Learning And Data Mining

Early data analysis techniques were oriented toward extracting quantitative and statistical data characteristics. These techniques facilitate useful data interpretations and can help to get better insights into the processes behind the data. Although the traditional data analysis techniques can indirectly lead us to knowledge, it is still created by human analysts (Michalski R. S. et al., 1998). A data analysis system has to be equipped with a substantial amount of background knowledge, and be able to perform reasoning tasks involving that knowledge and the data provided (Michalski R. S. et al., 1998). In effort to meet this goal, researchers have turned to ideas from the machine learning field. This is a natural source of ideas, since the machine learning task can be described as turning background knowledge and examples (input) into knowledge (output). If data mining results in discovering meaningful patterns, data is turned into information. Information or patterns that are novel, valid, and potentially useful are not merely information, but knowledge. One speaks of discovering knowledge, which was hidden before in the huge amount of data, but now revealed.

2.3 Supervised and Unsupervised Learning

The machine learning and artificial intelligence solutions may be classified into two categories: 'supervised' and 'unsupervised' learning. In supervised learning, samples of both fraudulent and non-fraudulent records are used. This means that all the records available are labelled as 'fraudulent' or 'non-fraudulent'. After building a model using these training data, new cases can be classified as fraudulent or legal (Jans M. et al., 2006). Furthermore, this method is only able to detect frauds of a type, which has previously occurred. In contrast, unsupervised methods don't make use of labeled records. These methods seek for accounts, customers, suppliers, etc. that behave 'unusual' in order to output suspicion scores, rules or visual anomalies, depending on the method (Bolton R. and Hand D., 2002).
Whether supervised or unsupervised methods are used, the output only gives us an indication of fraud likelihood. No stand-alone statistical analysis can assure that a particular object is a fraudulent one. It can only indicate that this object is more likely to be fraudulent than other objects (Jans M. et al., 2006). None of the above mentioned data analysis techniques have been found to be perfect for detecting fraud. They have been found to provide information about the likelihood of fraud. Hence, we have adopted the Ledger Assessment and Job Rotation technique so as to be able to preempt bank staff from perpetrating fraud while staying too long on a particular job.

3. CONCEPTUAL FRAMEWORK

The conceptual framework for the ledger assessment and job rotation technique is depicted in the figure 3.1 below.

![Conceptual Framework](image_url)

Job rotation involves shifting a person from one job to another, so that he is able to understand and learn what each job entails. In an organization such as a bank, job rotation should be carried out in order to prevent employees from committing any kind of fraud. For instance, if a person is handling a particular job for a very long time, there are tendencies for him to find loop holes in the system and then use them for his own benefit by indulging in fraudulent practices. Job rotation technique can be used to alleviate this problem. From the diagram of the conceptual framework, the transactions of the staff are monitored based on ledger assessment. If the ledger account is ok i.e. the account is balanced, then the job is rotated, then if the ledger assessment is not ok, then the staff will await a management decision which may be in form of sanction or penalty. If ledger assessment is ok, the staff’s job is rotated so that he/she does not stay too long on that job thereby acquiring some skills or detecting means of defrauding the bank due to mastery of that particular job.
4. DESIGN AND IMPLEMENTATION

Figure 4.1: Login Window for the Fraud Control System

Figure 4.2: User Registration Page

Figure 4.3: Transaction Entry Page
Figure 4.4: Ledger Assessment NOT OK

NOTE: This is just to assess the staff record. To check their transaction made for a job rotation. The maximum transaction a staff is expected to have made before his/her job rotation is 15 to 20. While the staff that falls below this wait for the management decision.

Figure 4.5: Ledger Assessment OK
5. RESULTS

Figure 5.1: SQL Result from the Database

Figure 5.2: Continuation of SQL Result
In order to implement, the fraud control system, 20 entries were made for members of staff of Cplus Bank. 12 members of staff whose ledger assessment was OK, had their jobs rotated while 8 staff members whose ledger assessment was not OK, have to await Management decision.

6. CONCLUSION

In support of the assertion made by Ekeiqwe C.C. (2000), another angle to fraud prevention is the adoption of computer aids as tool for fraud prevention and control. Good computer software will allow auditors to cover more grounds in less time and will also enhance the production of more accurate reports. This can be achieved by employing the computer programming technique known as ledger assessment and job rotation which was designed and implemented in this paper. Some of the advantages of this technique are that, it cannot be influenced by the bank management and the bank staff would not know when he or she is being monitored through ledger assessment process and when the job will be rotated.

REFERENCES