Fraud Detection in Instant Payments as Contribution to Digitalization in Banks

Alexander Diadiushkin[1,2], Kurt Sandkuhl[1,2] , Alexander Maiatin[2]

[1]University of Rostock, Albert-Einstein-Str. 22, 18059 Rostock, Germany
kurt.sandkuhl@uni-rostock.de
[2]ITMO University, St. Petersburg, Russia
dyadyushkin.a@yandex.ru

Abstract. Digitalization in banking has been an ongoing trend since many years aiming at automating most of the manual work in payment handling and integrating work flows of the involved service providers. The focus of the work presented in this paper is on fraud discovery and steps to fully automating it. Fraud discovery in financial transactions has become an important priority for banks. Fraud is increasing significantly with the expansion of modern technology and global communication, which results in substantial damages for the banks. Instant payment (IP) transactions cause new challenges for fraud detection due to the requirement of short processing time. The paper investigates the possibility to use artificial intelligence in IP fraud detection. The main contributions of our work are (a) an analysis of problem relevance from business and literature perspective, (b) a proposal for technological support for using AI in fraud detection of instant payment transactions, and (c) a feasibility study of the fraud detection approach.

Keywords: Artificial intelligence, enterprise modeling, digital transformation, instant payment

1 Introduction

Digitalization [21] opens up a variety of opportunities for changing business models and value chains in order to meet constantly increasing customer requirements and offer services faster, more intelligently and more efficiently. Many researchers consider Artificial intelligence (AI) as a core element of the ongoing digital transformation of enterprises [12]. However, among the prospective users of AI and the decision makers in organizations there is often no clear picture how AI should be put into operation and where the limits are. Digitalization in banking has been an ongoing trend since many years aiming at automating most of the manual work in handling banking products and services, which contributes to a transformation of the banking industry. The focus of this work is on fraud discovery and steps to fully automating it.

Fraud discovery in financial transactions has become an important priority for banks. Fraud is increasing significantly with the expansion of modern technology and global communication, which results in substantial damages for the banks and new

regulations. A new complexity in fraud detection is expected with the introduction of instant payment. European Central Bank and Central Bank of Russian Federation have already proposed such systems. Compared to conventional Single Europe Payment Area (SEPA) transactions, in instant payments fraud detection has to be completed within a few seconds instead of a day or more. New technological approaches are required to achieve this goal.

In the above context, the work aims at a contribution to quick fraud discovery by creating a library, which can be utilized in real-world fraud detection task. For this purpose, existing publicly available approaches were investigated to explore their utilization in the area of instant payments. One approach is selected for implementation with explicit focus on efficiency. To evaluate performance in terms of speed and precision, a benchmarking of this approach was performed.

The main contributions of our work are (a) an analysis of problem relevance from business and literature perspective, (b) a proposal for technological support for using AI in fraud detection of instant payment transactions, and (c) a feasibility study of a selected fraud detection approach. The remainder of this paper structured as follows: Section 2 summarizes the foundation for our work from fraud detection in payment transactions including important terms. Section 3 introduces the research approach taken. Section 4 investigates the problem relevance. Section 5 is dedicated to fraud detection and the feasibility study. Section 6 summarizes the results and gives an outlook on future work.

2 Theoretical foundation

2.1 Instant Payments

Originally, banks could take their time to process a payment transaction order. The procedure might take hours and even days. Formally, it consists of clearing and settlement of an order. Clearing is a process of transmitting, reconciling and, in some cases, confirming transfer orders prior to settlement. Settlement is the completion of a transaction or a processing with the aim of discharging participants' obligations through the transfer of funds [1].

To reduce the amount of time it takes to proceed with an order, European Central Bank and Central Bank of Russia developed the proposal of instant payment systems [4, 5]. Instant payments will dramatically increase the speed at which payments are made and received in Euro in the European Union. Today it normally takes one business day for a payment to reach the beneficiary. With instant payments this will happen in real time, 24 hours a day, 365 days a year. The funds will be available immediately for use by the recipient.

The Euro Retail Payments Board (ERPB) [6] has defined instant payments as "electronic retail payment solutions available 24/7/365 and resulting in the immediate or close-to-immediate interbank clearing of the transaction and crediting of the payee's account with confirmation to the payer (within seconds of payment initiation). This is irrespective of the underlying payment instrument used (credit transfer, direct debit or payment card) and of the underlying arrangements for clearing

(whether bilateral interbank clearing or clearing via infrastructures) and settlement (e.g. with guarantees or in real time) that make this possible."[4]

As described by Committee on Payments and Market Infrastructures [7], the idea of "instant" or sometimes called "fast" is not new. Technically, speed comes from instant clearing of the transaction, and only settlement process is being delayed. According to Mastercard [8], such approach is default for many countries but not for Europe and called Single-Message clearing, during which authorization and clearing in payment network is done in one dispatch. On contrary, Dual-Message clearing separates authorization and clearing processes in time [3].

2.2 Bank Fraud

Fraud is wrongful or criminal deception intended to result in financial or personal gain [9]. Thus, bank fraud is commonly described as a criminal act that occurs when a person uses illegal means to receive money or assets from a bank or other financial institution. Bank fraud is distinguished from bank robbery by the fact that the perpetrator keeps the crime secret, in the hope that no one notices until he has gotten away. The term bank fraud also refers to attempts by a person to obtain money from a bank's depositors by falsely pretending to be a bank or financial institution [10].

In the work, we focus on bank fraud cases, related to instant payment systems. Mainly, on identity thieves, stealing, duplication or skimming of card information, which may often be the result of phishing and Internet fraud. In other words, our main attention is on fraud approaches that utilize genuine payment card credentials.

In 2016, total fraud involving Single European Payment Area (also known as SEPA: the EU Member States plus Switzerland, Iceland, Lichtenstein and Norway) cards decreased to 1.8 billion euros, which is 0.8% less than in 2015. Card fraud at ATMs dropped by 12.4% and online fraud rose significantly, accounting for 73% of total value of card fraud in 2016. One Euro for every 2,428 Euros spent on payment cards was lost to fraud. In relative terms, i.e. as a share of the total value of card transactions of 4.38 trillion euros, fraud dropped by 0.001 percentage point to 0.041% in 2016, down from 0.042% in 2015. This is the first decrease since 2011 [11].

Online card fraud is naturally increasing as digital services develop further and is becoming more and more sophisticated. The most common types of online fraud reported by the industry are "clean fraud" – where criminals obtain genuine cardholder details including 3D Secure and Address Verification credentials – and "identity theft" – where the fraudster steals the cardholder's personal data in order to make unauthorized online transactions. However, in recent years there has been an increase in "friendly fraud", where the payer first makes a genuine transaction then claims that their card has been used fraudulently and asks for money back [2].

2.3 Fraud Discovery Approaches

In this section, an overview on related works found in public access is presented. In summary, more than 40 papers on fraud detection were analyzed in the process of

collecting related researches [13]. Quality highly varies between them; some even do not present any implementation or lack well-defined example of evaluation. Correlation to the banking fraud also divides into fraud in area of loan approvals and area of transactions, sometimes even datasets from one area applied for evaluation of approach for another, which seems to be not appropriate. A short overview on selected papers is presented below.

Vishwakarma et al. [23] propose an approach for fraud analytics for NFC-enabled mobile payment system. A multi-layer solution is presented where each subsequent layer is responsible for separated part of fraud analysis. However, paper presents only generic view on problem and its solution, avoiding implementation at all.

Kultur et al. [24] propose a novel cardholder behavior model for detecting credit card fraud. They propose building a model by clustering transaction amounts of a user, with respect to merchant category code (MCC) of the transaction, using Expectation Maximization algorithm. Evaluation was done on a real-world dataset provided by a leading bank in Turkey, which is not available in public. The proposed approach showed detection of 43% of fraud transactions, presented in the dataset. However, no information about application of this approach in real world were provided.

Carminati et al.[25] propose a supervised auto-tuning approach for a banking fraud detection system, called Banksealer [17]. They describe application of Multi-Objective Genetic Algorithm (MOGA) for task of feature weighting task, this way freeing end users from need in manual configuration of this unsupervised system. This gain up to 35% of performance in detecting some sophisticated fraud cases.

Patil et al. [26] implemented supervised artificial neural network with back propagation algorithm for purpose of classifying transactions for fraud detection. Experimental evaluation was made on old dataset of applications for credit loans, what seems to be unrelated to the task of fraud detection in bank transactions. However, accuracy up to 98% was shown during evaluation.

Hatamikhal et al. [27] present concept drift detection solution based on streaming ensemble algorithm with deep belief network utilized in it. Concept drift problem highly affects fraud detection due to variable user's behavior. Evaluation was done on MNIST and SEA datasets, comparing proposed solution with Morelli's method. The F1-score of proposed method for the evaluation is 50.41%.

Nami et al. [28] developed two-stage approach for fraud detection. In the first stage, kNN algorithm utilized to rate similarity between past user's transactions and incoming ones. In the second stage, dynamic random forest algorithm was applied for initial detection along with the minimum-risk model for cost-sensitive fraud detection. Evaluation was made on data from private bank and future deployment in real world is only proposed for research.

Panigrahi et al. [29] build fraud detection systems, which combine several approaches. Initially, proposed approach checks for address mismatch and detects outliers using DBSCAN algorithm. Afterwards, results of previous checks are combined using Dempster-Shafer adder. If the result falls into certain threshold, additionally Bayesian learner applied to make optimal decision. Evaluation was done on synthetic dataset with up to 98% of true positive cases and less than 10% of false positive ones. No information about future application in real world is presented.

3 Research approach

The overall research paradigm we follow in our work is design science research (DSR) as proposed by [22]. The research goal is to investigate the potential of using AI as element in digitization of fraud detection in instant payments (IP) with a focus on requirement analysis and feasibility study. The artefact envisioned as long-term result and thus in focus of our DSR project is a method support for introducing AI in IP fraud discovery in combination with technological components implementing AI approaches.

Within the DSR frame, we use different research methods in different phases of the research work. Problem relevance is investigated by an interview study in different banks and financial service providers (see section 4). This business-oriented aspect of the problem relevance is accompanied by a literature analysis to discover relevant existing work in the scientific body of knowledge (see section 2). The main research questions of the problem relevance investigation are "What challenges do organizations in the financial industry experience in implementing fraud detection in instant payments?".

Based on the problem relevance, we derive requirements and propose an initial design of the envisioned technological support, i.e. the AI component. This initial version serves as a feasibility study for fraud detection in instant payment transactions applying AI. Lessons learned from the feasibility study and requirements derived from the interviews form an input for the next design-evaluate cycle of the artefact. The initial version of the method is not discussed in this paper but presented in related work [14].

4 Problem Relevance

The investigation of problem relevance was performed in two steps: first, we performed interviews with three different payment service providers about their way of performing fraud detection in conventional SEPA payments. In the second step, we analyzed the payment handling in a company offering IP clearing services.

The interviews were conducted on the basis of a structured questionnaire. Objective of the interviews was to understand which steps in conventional SEPA fraud detection could no longer be performed in instant payment fraud detection because of the short time frame. In SEPA payments, banks usually have one bank day for fraud detection, in instant payments max. 10 seconds. Thus, the interviews aimed at gaining a better understanding of the process of processing suspected cases. For the analysis of the suspected case, the manual process receives or fetches different information:

- Reason for displaying the suspicious case, e.g. known suspicion / fraud pattern, rule(s),
- assessment result of the criticality of the suspected case, e.g. using multi-level scale,
- Information about the triggers of the transaction, for example name, age, address data; transaction / sales history,

- Information about the content and recipient of the transaction, such as account information of the trigger, amount, intended use, name and bank details of the recipient,
- Any further information about the trigger of the transaction, such as the service agent in the bank assigned to the customer.

The basic process flow of fraud detection takes an average time for the manual parts between 5-10 minutes and up to 30 minutes for difficult cases.

The payment service provider is a small company from Germany offering clearing layer and settlement layer functions, as well as value-added services, such as sanction screening and embargo checking, for small and medium-sized banks. The company is one of the first in Germany to offer support for instant payment transactions. Motivated by a report of a Danish payment service using machine learning for fraud detection in domestic real-time payments in Denmark, the case study company decided to explore possibilities of AI use of IP in their own services. Currently, the fraud detection in IP is performed using a rule-based approach, which is not fully suitable to automate the manual steps discovered in the interview study.

5 Feasibility Study: Fraud Detection in IP based on AI

Section 2.3 shows that there are many fraud detection approaches but that publications describing these approaches do not provide sufficient information for using or implementing them. Thus, we decided to apply a general approach, i.e., for the feasibility study, the use of a random forest approach was selected.

5.1 Random Forest

Random Forest is an ensemble classifying algorithms that represents ensembles a collection of Decision Trees, each of which is built on a randomly selected set of features. A decision tree is a tree where each node represents an attribute and edges following from it represent a condition, under which the edge can be traversed. On leafs of the tree target classes are located. The final decision is represented by majority of results. It is easy to see that model behind Random Forest can be easily visualized and analyzed for investigation, thus, results of classification can be explained in reasonable amount of time.

Methods for creation of Random Forest mainly consist of three approaches: bagging, random split and random set of weights. Bagging is made by sapling original training data set randomly, until certain size is reached. This way, training data sets made by bagging may contain duplicates. For random splitting, a tree is built using K attributes from training data set, selected at random. Last approach is similar to bagging but duplicates are represented by weighting of instances – the more instance's weight, the more copies of it were sampled.

A decision is made by traversing the tree from root to leaf by a path that meets conditions associated with it. In the end, arriving to a leaf presents the result of classification process. Random Forest runs classification on each tree it consists of during the runtime.

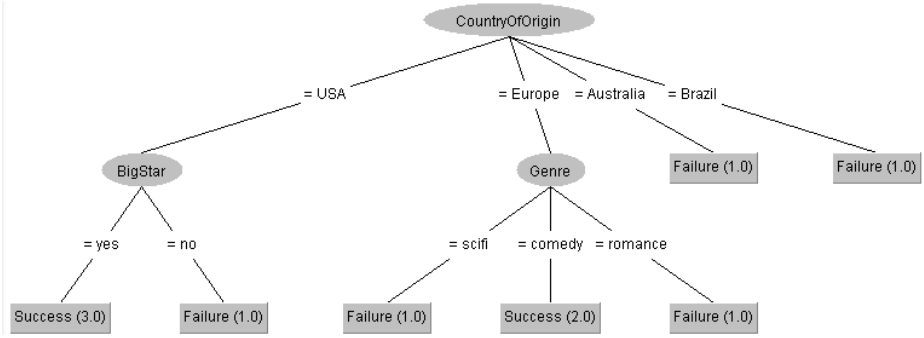

Figure 1 - Example of Decision Tree visualization

5.2 Implementation

For evaluation purpose, only the data set from Kaggle [19] was utilized in this work. The reason for this decision is that it consists of real-world transactions, ready to be utilized in classification algorithm. Disadvantage of this data set is high anonymity, thus, it can't be utilized fully for certain algorithms as they require some knowledge of users. Features, presented in this data set include the following information:

- Time – between current transaction and first transaction in the data set,
- V1-V28 – anonymized features of transaction,
- Amount – transaction amount,
- Class – nominal attribute that classifies transaction as fraudulent or not.

Since information about users is vital for correct evaluation of algorithms, it is necessary to look for synthetic data. Only one suitable simulator of bank transactions was found: PaySim [20].

For Random Forest, implementation from WEKA [15] was chosen, as will be demonstrated further. WEKA is probably the most popular, open-source, production-ready library, that provide support of many algorithms. It supports many data formats and even connection to SQL databases via JDBC. Official GUI allows experimenting and result visualization without the need for a single line of code, just like similar commercial products, for example, RapidMiner. There are three main approaches to build Random Forest classifier: bagging, random split and random weighting. WEKA implementation of the algorithm supports combining of first and last approach with random split.

Since parametrization of this algorithm may vary depending on incoming data, it is necessary to create generic classification detector for high customization and de-duplication purpose. Generic interface for classifiers in WEKA is called Classifier. Source data in WEKA presented as a collection, named Instances, each of which is presented by interface Instance. Data attributes are represented by the attribute class. Figure 2 shows the class diagram of generic classifier detector implementation, which was part of the implementation.

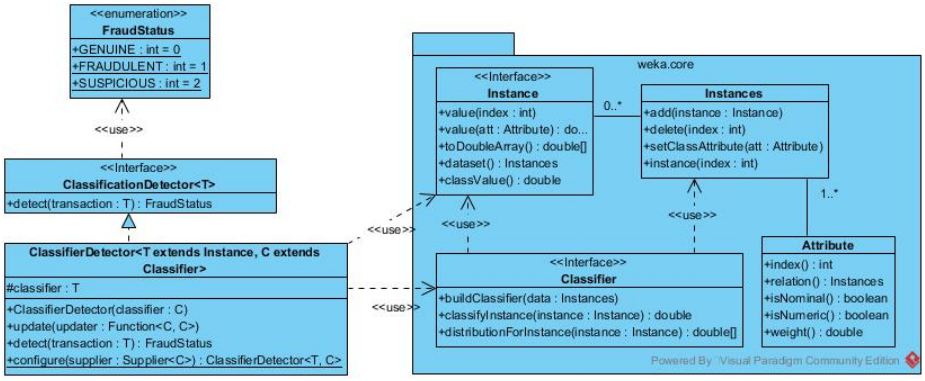

Figure 2 - Class diagram of generic classifier detector implementation

Further in implementation, Instances, Instance and Attribute were used for storing and handling of data. Rich set of operations can be performed with Filter class, which makes it easy to manipulate large amounts of data without need in manual implementation with aforementioned classes and interfaces.

5.3 Evaluation

For initial unit testing of different algorithms' implementation and for testing assumptions about their performance the Junit [16] library was utilized. For benchmarking purpose, JMH [17] from OpenJDK were applied. A plugin for Gradle [18] allowed run benchmarking process as simple as possible. Different metrics can be extracted during evaluation but since detection must fit into certain amount of time, operation per second is the one that was used.

Since it is unknown whether Random Forest model must be built for each user separately or can be global, the first approach was assumed. Loading of data is separated from benchmark evaluation into the setup, since implementation mainly requires only vector of float point numbers, so transformation into this representation would depend on actual data source. In addition, building a detector and actual detection always spited into different benchmarks. Typically, 10 iterations of building process and 50 iterations of detection were benchmarked. For purpose of precision evaluation, Fβ-scores were calculated with $\beta = 1$ and $\beta = 2$

Results of the evaluation

Evaluation was performed on transaction data set, generated by modified version of PaySim. This data set contained around 15 thousand transactions, more than 600 of which were fraudulent and 450 clients were involved in the simulation.

Performance measure was performed by 5 benchmarks, each of which were executed 101 number of iterations with 5 iterations of warm-up. Evaluation was performed on typical PC-class machine with 16 GB of RAM and Intel® Core™ i5-3450.

Since global profile of user is derived from payee of a transaction and represented by a single score, it can be derived outside the detector. Since resulting score is a

multiplication of all scores and amount value, it is correct to assume that detection time for global profile is constant, as it only depends on how results of the profile creation are stored.

Table 1 – Result of the evaluation

	Random Forest	Computing Platform
Building (sec)	0.003170	PC-class machine with 16 GByte of RAM and Intel® Core™ i5-3450
Detection (sec)	0.000003	
Fβ-score(β=1)	0.950	
Fβ-score(β=2)	0.926	
Fβ-score(β=3) weighted average	0.987	

6 Conclusions

In this work, current state of fraud detection area was researched and overviewed. Limitations of the research area and existing approaches were presented. The biggest limitation currently is the lack of real-world test data which can be used for developing and evaluating fraud detection approaches.

Based on the observations and analysis results of the problem analysis presented in section 4, we argue that there is a need for additional technology support for fraud discovery in instant payments and propose an AI implementation using random forest approach. To overcome unavailability of proper testing data, a modification of existing payment simulator was proposed and implemented. This allowed successful evaluation of the explored approach.

The selected approach was efficiently implemented and tested for ability to be applied in instant payments area. As an artifact, a programming library that provides this approach for further production use was designed and implemented.

Further research can be done by improving the library with other production-ready approaches. In addition, area of payment simulators can be improved to generate more suitable transactions for different kinds of payment methods. This would allow gathering more useful context information that can slightly improve the quality of detection process.

Acknowledgements

The research presented has been supported by Government of Russian Federation, Grant 08-08 and by German International Exchanges Agency (DAAD), Grant 57464138.

References

[1] European Central Bank, 'Glossary of terms related to payment, clearing and settlement systems', 2009. [Online]. Available: https://www.ecb.europa.eu/pub/pdf/other/glossaryrelatedtopaymentclearingandsettlementsystemsen.pdf.

[2] Mastercard Incorporated, 'MASTERCARD INCORPORATED - FISCAL YEAR 2017 FORM 10-K ANNUAL REPORT', 2017. [Online]. Available: https://www.sec.gov/Archives/edgar/data/1141391/000114139118000009/ma12312017-10xk.htm. [Accessed: 01-Apr-2019].

[3] Bank for International Settlements, 'Clearing and Settlement Arrangements for Retail Payments in Selected Countries', 2000.

[4] European Central Bank, 'Instant Payments', 2019. [Online]. Available: https://www.ecb.europa.eu/paym/retpaym/instant/html/index.en.html.

[5] Банк России, 'Система быстрых платежей', 2019. [Online]. Available: https://www.cbr.ru/psystem/sistema-bystrykh-platezhey/.

[6] European Central Bank, 'Euro Retail Payments Board'. 2019.

[7] Committee on Payments and Market Infrastructures, 'Fast payments - Enhancing the speed and availability of retail payments', 2016.

[8] S. Herbst-Murphy, 'Clearing and Settlement of Interbank Card Transactions: A MasterCard Tutorial for Federal Reserve Payments Analysts', 2013.

[9] Oxford English Dicttionary, 'Fraud', 2019. [Online]. Available: https://en.oxforddictionaries.com/definition/fraud.

[10] Legal Dictionary, 'Bank Fraud', 2019. [Online]. Available: https://legaldictionary.net/bank-fraud/.

[11] European Central Bank, 'ECB report shows a fall in card fraud in 2016', 2018. [Online]. Available: https://www.ecb.europa.eu/press/pr/date/2018/html/ecb.pr180926.en.html.

[12] Rifkin, J. (2013) The Third Industrial Revolution: How Lateral Power Is Transforming Energy, the Economy, and the World. St. Martin's Griffin. Available at: https://www.amazon.com/Third-Industrial-Revolution-Lateral-Transforming/dp/0230341977.

[13] Diadiushkin, Aleksandr (2019) Automation of transaction analysis for fraud detection in instant banking payments. Master thesis in study program Business Information Systems. Institute of Computer Science, University of Rostock, June 2019.

[14] Sandkuhl, Kurt (2019) Putting AI into Context - Method Support for the Introduction of Artificial Intelligence into Organizations. CBI (1) 2019: 157-164. IEEE.

[15] WEKA (2019) WEKA: RandomForest, 2019. [Online]. Available at: http://weka.sourceforge.net/doc.dev/weka/classifiers/trees/RandomForest.html.

[16] Junit (2019) JUnit 4, 2019. [Online]. Available at: https://junit.org/junit4/.

[17] OpenJDK (2019) OpenJDK: jmh, 2019. [Online]. Available at: https://openjdk.java.net/projects/code-tools/jmh/.

[18] C. Champeau (2019) JHM Gradle plugin, 2019. [Online]. Available at: https://github.com/melix/jmh-gradle-plugin.

[19] Machine Learning Group - ULB, 'Credit card fraud detection', 2016. [Online]. Available: https://www.kaggle.com/mlg-ulb/creditcardfraud.
[20] E. Lopez-Rojas, A. Elmir, and S. Axelsson, '3 Paysim : A financial mobile money simulator for fraud detection', 28th Eur. Model. Simul. Symp. EMSS 2016 , 2016.
[21] Matt, C., Hess, T., & Benlian, A.: Digital transformation strategies. Business & Information Systems Engineering, 57(5), 339-343 (2015)
[22] Peffers, K., Tuunanen, T., Rothenberger, M.A., Chatterjee, S.: A design science research methodology for information systems research. Journal of Management Information Systems 24, 45–77 (2007)
[23] P. Vishwakarma, A. K. Tripathy, and S. Vemuru, 'A Layered Approach to Fraud Analytics for NFC-Enabled Mobile Payment System', Lect. Notes Comput. Sci., vol. 10722, pp. 127–131, 2018.
[24] Y. Kultur and M. Çağlayan, 'A Novel Cardholder Behavior Model for Detecting Credit Card Fraud', Intell. Autom. Soft Comput., vol. 24, no. 4, pp. 808–817, 2018.
[25] M. Carminati, L. Valentini, and S. Zanero, 'A Supervised Auto-Tuning Approach for a Banking Fraud Detection System BT - Cyber Security Cryptography and Machine Learning', 2017, pp. 215–233
[26] P. S. Patil and N. V. Dharwadkar, 'Analysis of banking data using machine learning', in Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2017, 2017.
[27] N. Hatamikhah, M. Barari, M. R. Kangavari, and M. A. Keyvanrad, 'Concept Drift Detection via Improved Deep Belief Network', in 26th Iranian Conference on Electrical Engineering, ICEE 2018, 2018.
[28] S. Nami and M. Shajari, 'Cost-sensitive payment card fraud detection based on dynamic random forest and k-nearest neighbors', Expert Syst. Appl., 2018.
[29] S. Panigrahi, A. Kundu, S. Sural, and A. K. Majumdar, 'Credit card fraud detection: A fusion approach using Dempster-Shafer theory and Bayesian learning', Inf. Fusion, 2009.