

Architecture of Transaction Monitoring System of Central Banks

Scenario Probabilistic Logic Models for Detecting Fraud Activity via Payment Systems of Central Banks

Maxim Repin

Dept. of Information Security, IU8
Bauman Moscow State Technical University
Moscow, Russian Federation
bmstu.iu8@gmail.com

Oleg Mikhalsky

Dept. of Information Security
Moscow Polytechnic Institute
Moscow, Russian Federation
o.o.mikhalsky@mospolytech.ru

Ekaterina Pshehotskaya

Dept. Information Security
Moscow Polytechnic Institute
Moscow, Russian Federation
pshehotskaya@gmail.com

Abstract— The detection of fraud payments is one of the primary problems for cyber-security of payment services. Among all services, the exclusive ones are the payment systems of central banks regarding their critical role for financial systems, sheer volume and number of transactions and increased attention from perpetrators. One of the main mechanisms providing detection of fraud operations within interbank netting and settlement payments is a transaction monitoring system. These systems including their complexity and use-case specifics can be represented via probabilistic logic models, considered in this paper. The complete transaction monitoring system comprises several distinct algorithmic modules, which perform tiered checks for conducted payments. To increase adaptability to new types of fraud, the system architecture includes a module of model correction that allows one to detect new threat patterns and to adjust appropriate response while keeping false-positive alerts at low level.

Keywords— *payment system; information security monitoring; probabilistic logic models; information security risks; initiating events*

I. INTRODUCTION

As a rule [1-3], detection of fraud activity on running payment system is implemented via analysis of transaction flow as well as automated analysis and accounting of history of incidents, revealed by respective actors of the payment system.

Payment systems of central banks have the unique feature that their clients are banks and other credit institutions, but not the physical entities. This feature is reflected in both specifics of operation and special set of risk indicators that can imply ongoing fraud transaction. Moreover, the similar payment

systems frequently fall under requirements to minimize transaction timeframe, which significantly complicates the analysis of risk indicators.

The general operation principle of the transaction monitoring system (TMS) for central banks can be represented in a conceptual scheme in Fig.1.

The key features of scheme on fig. 1 are:

a) A two-tier scheme of operation processing. Fast processing allows checking payments on-the-fly, not affecting designed characteristics of transaction monitoring system, like performance of payment processing. Full processing provides operator-driven assessment of earlier withdrawn of dubious transactions from batch payments, and additional analysis of payments via special models.

b) Suspension and detailed analysis of specified dubious payments by a request of a payment system client, or in case of credible apprehensions.

c) Notification of payment system participators on the detection of fraud payments inferred from the results of full processing augmented by the opinions of analytics in the transaction monitoring system.

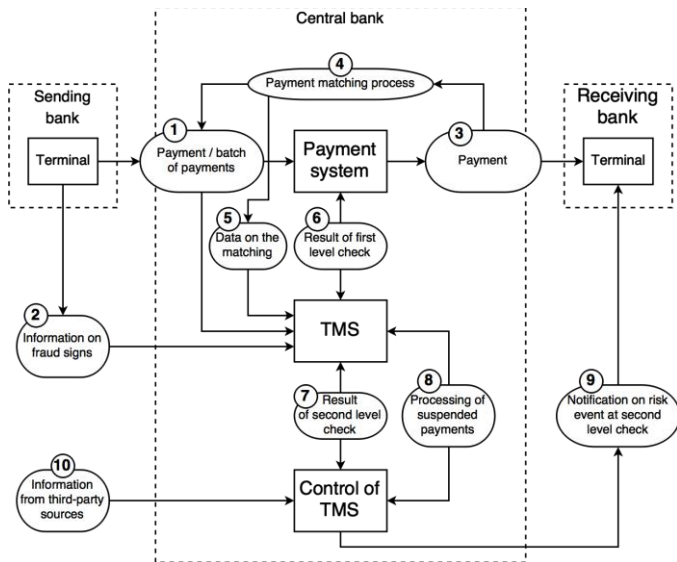


Fig. 1. Conceptual scheme for general operation principle of transaction monitoring system. 1 – receipt of payment/batch of payments from a participant of payment system; 2 – information on fraud signs from a participant; 3 – dispatch of payment information to payment recipient; 4 – comparison of conducted transactions with clients-submitted payment orders; 5 – submission of comparison results into transaction monitoring system; 6 – submission of decision on fraud/legitimate nature of operation into transaction monitoring system, withdrawal of high risk payments; 7 – receiving offline checking results; 8 – resolution of operator-expert of transaction monitoring system on confirming/disapproving of potential fraud, return of earlier withdrawn payments into processing in latter case; 9 – notification dispatch to the participant with detected potential fraud operations; 10 – dispatch of the information from third-party sources on possible fraud actions including information on compromised banking infrastructure into transaction monitoring system.

The presented scheme is to be embedded into payment processing structure as an additional method for verification of payment or batch of payments.

To analyze payment data, it is necessary to determine a quantitative coefficient for risk value of fraud occurrence, which is calculated based on coupled indicators.

Fraud analysis methods can be formally divided into following categories:

- analysis rules, common for all processed payments;
- analysis rules, acting in the content of scenarios formed for abnormal situations [4,5];
- analysis carried out with correctable scenario probabilistic logic models.

Therefore, the architecture for TMS should allow not only conducting analysis of explicitly detected fraud, but also estimating inter-relations between indicators.

The modular logical architecture of TMS permits its functional description with probabilistic logic models. The special aspects of their use and logical architecture are considered in the following section.

II. ARCHITECTURE OF TRANSACTION MONITORING SYSTEM

In general case, the logic architecture of TMS can be formed from following modules:

- real-time module of common check rules (CCR);
- real-time module of profiled check rules (PCR);
- regular-run module of correctable probabilistic logic model (CPLM);
- regular-run module of post-processing checks (PPC);
- regular-run module of evaluating model correction and corrective measures (MMC).

The logical structure of TMS is presented in Fig.2.

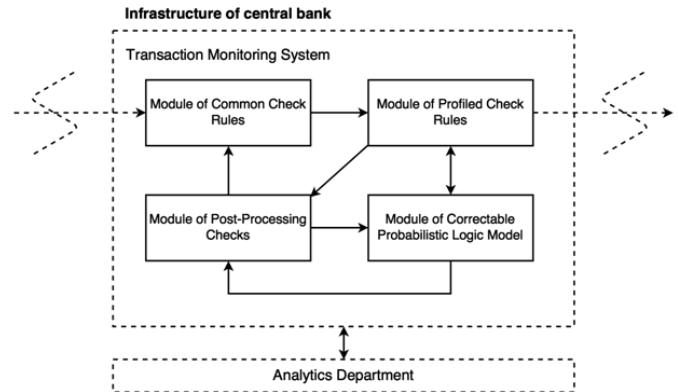


Fig. 2. The logical structure of TMS

A. Probabilistic Logic Model of TMS

Let $M = \{m_1, \dots, m_n\}$ be the set of TMS modules. The probability to detect fraud (unsuccessful payment processing) Y depends on the result, returned by each module. Thus, the probabilistic logic model of the fraud in the payment system has the following description: the fraud can be detected by a single module or by any two modules or by any combination of modules. Then, the probabilistic logic model of payment legitimacy control can be expressed as:

$$Y = Y_1 \vee \overline{Y_2} \vee Y_3 \vee Y_4,$$

where

- Y_1 is detection event for CCR-module;
- Y_2 is detection event for PCR-module;
- Y_3 is detection event for CPLM-module;
- Y_4 is detection event for PPC-module.

The probability function of successful payment processing can be described as:

$$\{Y\} = P_1 + P_2(1 - P_1) + P_3(1 - P_2) + P_4(1 - P_3),$$

where P_1, P_2, P_3, P_4 are the respective probabilities of payment fraud detection by each module.

Next, let us consider the functionality of each module in more detail.

B. Module of Common Check Rules Y_1

The module of check of common rules is a body of rules, providing the check in accordance with the data on transactions conducted earlier. This module uses earlier specified examination scenarios for objects that do not have individual profiles for fraud analysis.

Let $F = \{f_1, \dots, f_n\}$ be the set of payment characteristics, $S = \{s_1, \dots, s_m\}$ be the set of fraud scenarios, containing specified payment characteristics. To facilitate fraud analysis, it is reasonable to group payment characteristics with respect to common specific features that are mutually exclusive for different subsets. For example, such features are the payment conditions or class of the payment system participator. So, the set of payment characteristics can be written in the following form:

$$F: f_1 = \{f_{1'}, \dots, f_{q'}\}; \dots f_n = \{f_{n1'}, \dots, f_{nz'}\}.$$

Then, the flowchart of fraud detection can be represented as follows:

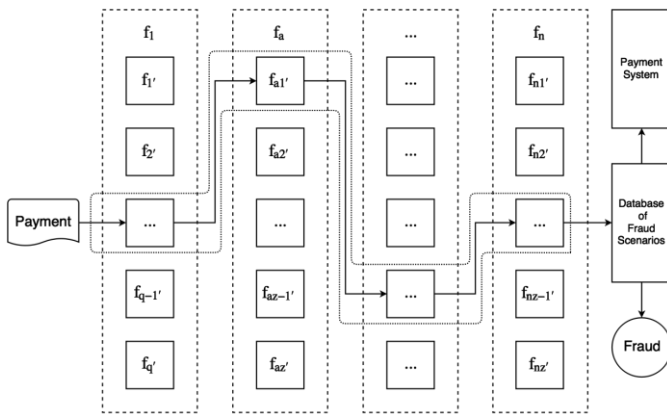


Fig. 3. Flowchart of fraud detection

In general case, the rules of this module are based on the best practices of fraud detection and expert evaluations. Additionally, the functioning of the module allows corrections based on the data generated by a post-processing module.

The resulting description of the probabilistic logic model is as follows:

$$Y_1 = Y'_1 \vee Y'_2 \vee Y'_3 \vee \dots \vee Y'_n,$$

where $Y'_1, Y'_2, Y'_3, \dots, Y'_n$ are the fraud scenarios;

$$Y'_n = Z_1 \wedge Z_2 \wedge \dots \wedge Z_m,$$

where Z_1, Z_2, \dots, Z_m are the payment characteristics, which simultaneous presence indicates of fraud signs.

C. Module of Profiled Check Rules Y_2

The module of profiled checks is a body of check rules carried out with respect to the behavioristic model of analyzed entities. The behavioristic model (the profile) represents a set of typical behavioristic patterns accounting for individual characteristics of payment system participators and their clients [6]. The profiles are formed, based on existing history of operations.

The module operates with the following types of profile:

- sender account;
- receiver account;
- class of sender account;
- class of receiver account;
- sending bank;
- receiving bank;
- class of sending bank (class of payment system participator);
- class of receiving bank (class of payment system participator);
- class of payment conditions.

Profiles of a sender account class in the context of the participator bank are formed for use in operation checks of previously unexamined accounts. Account profiles are formed considering the type of the committed operation (payment conditions) to allow the analysis of information on technological aspects of payment, e.g. a payment category, a purpose of payment and so on. The profiles are based on the history of operations obtained while forming respective classes, and are formed on different hierarchical tiers. During the analysis of payments on the fraud signs, the rules with more detailed profiles have the priority.

Therefore, unlike the module of common check rules, the module of profiled checks contains the rules to validate specified participators of the payment system considering unique aspects of their payments. Then, $F1 = \{F_{11}, \dots, F_{1q}\}$ describes the set, containing the subsets of all payments, distinctive to the unique participator.

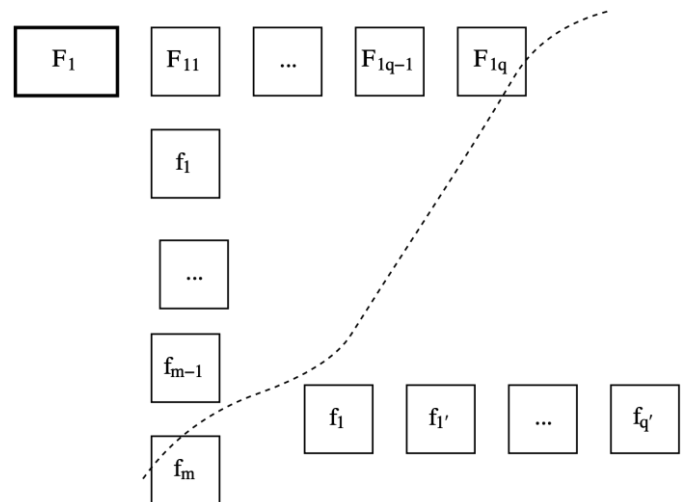


Fig. 4. Flowchart of payment validation rules for specified participator of payment system

The probabilistic logic model of the CPLM-module can be expressed as:

$$Y_2 = Y'_1 \vee Y'_2 \vee Y'_3 \vee \dots \vee Y'_m,$$

where $Y'_1, Y'_2, Y'_3, \dots, Y'_m$ are the payment scenarios of payment system client, and

$$Y'_m = Z_1 \wedge Z_2 \wedge \dots \wedge Z_m,$$

where Z_1, Z_2, \dots, Z_m are payment characteristics. The payment characteristics can be expanded into greater detail, e.g.

$$Z_1 = K_1 \wedge K_2 \wedge \dots \wedge K_k,$$

where K_1, K_2, \dots, K_k are detailed characteristic of payment. It is worth noting that as opposed to CCR-module, the PCR-module uses the scenarios of legitimate payments, so the resulting probabilistic logic model of TMS has the inversed value of Y_2 .

D. Module CPLM Y_3

First, let us introduce the parameter of integrity for payment system clients A . Let $A = A_f/A_y$, where A_y is the total number of client payments per year, A_f is the number of client payments per year under apprehension. Thus, new clients have weight $A = 1$. Also, the tuning of TMS should include the threshold value of parameter A .

The CPLM-module is based on the sets of characteristics of client payments and sets of fraud scenarios. The databases for the CPLM-module correspond to the same profiles of the module of profiled checks. The complete list of types used to detect fraud client operations contains:

- sender account;
- receiver account;
- class of sender account;
- class of receiver account;
- sending bank;
- receiving bank;
- class of sending bank;
- class of receiving bank.

The correctable probabilistic logic models of sender and receiver account classes are built to check operations on accounts not encountered earlier with respect to weight characteristic of a client. These probabilistic logic models are corrected based on the history of operations accumulated in the process of forming respective account invoices.

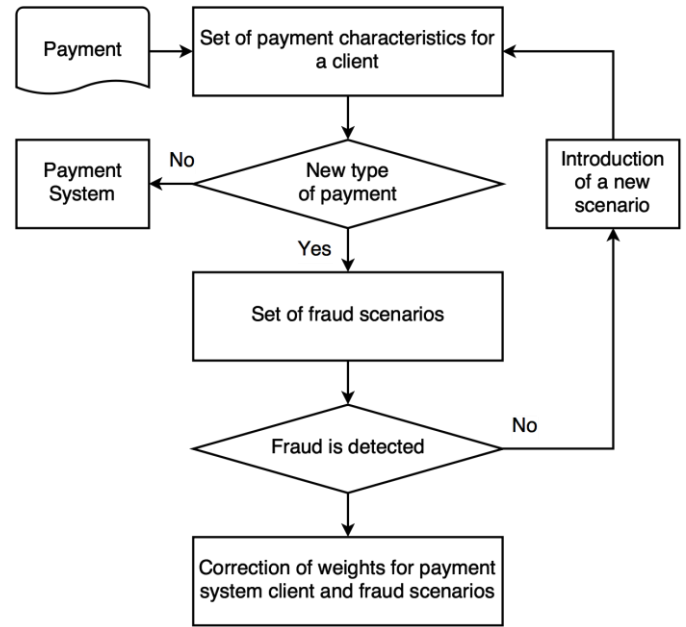


Fig. 5. Flowchart of CPLM-module

The probabilistic logic model of the CPLM-module is analogous to the model of profiled checks except the function of adding client payment scenarios. If payment characteristics mismatch all known payments of the considered client, these characteristics are compared with records of fraud signs in the database. To detect new fraud scenarios, it is necessary to enumerate combinations of existing scenarios. Then, $Y_3 = Y'_1 \wedge Y'_2 \vee Y'_1 \wedge Y'_3 \vee Y'_2 \wedge Y'_3 \vee Y'_1 \wedge Y'_2 \wedge Y'_3 \dots \vee Y'_n$ are the combination of fraud scenarios, where $Y'_1, Y'_2, Y'_3, \dots, Y'_n$ are fraud scenarios, and $Y'_n = Z_1 \wedge Z_2 \wedge \dots \wedge Z_m$, where Z_1, Z_2, \dots, Z_m are payment characteristics, which simultaneous presence implies the fraud signs.

E. Post-check Module Y_4

The PC-module is used to reveal relations between different accounts based on several criteria including not only behavioristic specifics of account holders. This module proceeds checking the transactions conducted within a specified timeframe. Account relations detected by the post-check module provide corrections of common check rules of the corresponding CCR-module.

The post-checks are carried out similarly to an approach of control actions [7]. The control action is represented by additional information, so that the set of payment characteristics complemented with it will have fraud signs. The probabilistic logic model of the PCR-module can be expressed via the probabilistic logic models of operational risk [8-11]. These models define control actions as additional events Y_z, Y_A, Y_p, Y_{SNS} at the levels of payment characteristics, detailed payment characteristics, and fraud scenarios. Then, $Y_4 = Y''_1 \vee Y''_2 \vee Y''_3 \vee \dots \vee Y''_m$, where $Y''_1, Y''_2, Y''_3, \dots, Y''_m$ are the corrected payment scenarios, and $Y''_m = Y'_m \wedge Y_{pm}$, where Y'_m is a client payment scenario. The correcting action results in expression $Y'_m = Z_1 \wedge Z_2 \wedge \dots \wedge Z_m \wedge Y_z$. By analogy,

similar actions can be included in models of detailed payment characteristics and scenario models.

F. Module of Model Corrections

By nature of business development of participator banks, the profiles based both on rules and CPLM-methods degrade in time. Moreover, new fraud scenarios emerge, so there is a necessity to form new corresponding profiles. To maintain the performance, regular relearning of TMS is required.

The significant factor of proper TMS relearning is the feedback from participator banks and other financial organizations. The most crucial aspect of such feedback is the consideration of false-positive cases.

The relearning of TMS proceeds in several stages and accounts for:

- a list of participator-confirmed fraud operations;
- an inflow of new data;
- revealing of new significant factors during additional analysis.

III. CONCLUSION

The article presents the model of the transaction monitoring system serving as a base for the proposed structural probabilistic logic model of fraud detection in payment systems of central banks. The proposed TMS-model is a complex solution providing fraud detection by the use of several modules that implement various methods of payment analysis in real-time environment.

Using the singular or group-wide profiles, the TMS provides accounting for special features of payment processing. Both types of profiles are implemented to check payments via the module of profiled checks as well as the module of correctable probabilistic logic models. The TMS retains its ability to detect fraud due to regular retraining. Such retraining allows one:

- to maintain the fraud detection efficiency level;

- to detect targeted attacks on partner-banks infrastructure;
- to match actual threats.

The probabilistic logic model of TMS allows one to describe complex dependencies between analyzed entities (payment characteristics, payment scenarios, fraud scenarios and so on), as well as the relation between them and additional fraud indicating data. The use of probabilistic logic models to govern processes of fraud detection facilitates the exclusion of uncertainties that emerge during estimation of potential fraud signs.

References

- [1] A. Sizov, "Main functions of counter-fraud system," Jet-Info, no. 7, 2014.
- [2] "Fraud Detection and Prevention: Transactional Analysis for Effective Fraud Detection," ICL Whitepaper, WP/FD/110106, p. 12, 2006.
- [3] B. Pushpalatha, and C. Willson Joseph, "Credit Card Fraud Detection Based on the Transaction by Using Data mining Techniques," IJRCCE, vol. 5, no. 2, 2017.
- [4] M. Repin, "Risk models of information security violations in the payment system," RSUH/RGGU BULLETIN, no. 3(5), pp. 90-94, 2016.
- [5] O. Kazarin, and M. Repin, "Security state model of the payment system," RSUH/RGGU BULLETIN, no. 3(5), pp. 81-89, 2016.
- [6] R. Devaki, V. Kathiresan, and S. Gunasekaran, "Credit Card Fraud Detection using Time Series Analysis," International Conference on Simulations in Computing Nexus, ICSCN-2014, International Journal of Computer Applications®(IJCA). 2014.
- [7] M. Repin, "The model risk management of information security in payment system," Information and innovations, no. 1, pp. 102-105, 2016.
- [8] E.D. Solozhentsev, "Scenario probabilistic logic risk management in business and engineering," Saint Petersburg. Buisness-press publishing house, p. 432, 2004.
- [9] E.I. Karaseva, and A.G. Stepanov, "LP Operational Risk Model in Banking," Information-control systems, no. 2, pp. 77-83, 2011.
- [10] M.A. Bukhtin, "Technique and practice for operation risks management in commercial bank," Moscow, workshop of Insitute of banking business of Russian banks association, Moscow, 27.03 — 28.03.2009.
- [11] B.V. Sazykin, "Managment of operation risk in commercial bank," Moscow, Vershina publishing house, p.272, 2008.