DOI: 10.15276/aait.01.2021.3
UDC 004.89

DEVELOPMENT OF THE AUTOMATED FRAUD DETECTION SYSTEM CONCEPT IN PAYMENT SYSTEMS

Iuliia L.Khlevna[1)]
ORCID: http://orcid.org/0000-0002-1807-8450; yuliya.khlevna@gmail.com
Bohdan S. Koval[1)]
ORCID: http://orcid.org/0000-0002-3757-0221; bohkoval@gmail.com
[1)]Taras Shevchenko National University of Kyiv, Volodymyrska str., 60, Kyiv, 01033, Ukraine

ABSTRACT

The paper presents the demand for the spread of payment systems. This is caused by the development of technology. The open issue of application of payment systems - fraud - is singled out. It is established that there is no effective algorithm that would be the standard for all financial institutions in detecting and preventing fraud. This is due to the fact that approaches to fraud are dynamic and require constant revision of forecasts. Prospects for the development of scientific and practical approaches to prevent fraudulent transactions in payment systems have been identified. It has been researched that machine learning is appropriate in solving the problem of detecting fraud in payment systems. At the same time, the detection of fraud in payment systems is not only to build the algorithmic core, but also to build a reliable automated system, which in real time, under high load, is able to control data flows and effectively operate the algorithmic core of the system. The paper describes the architecture, principles and operation models, the infrastructure of the automated fraud detection mechanism in payment systems. The expediency of using a cloud web service has been determined. The deployment of the model in the form of automated technology based on the Amazon Web Services platform is substantiated. The basis of the automated online fraud detection system is Amazon Fraud Detector and setting up payment fraud detection workflows in payment systems using a customizable Amazon A2I task type to verify and confirm high-risk forecasts. The paper gives an example of creating an anomaly detection system on Amazon DynamoDB streams using Amazon SageMaker, AWS Glue and AWS Lambda. The automated system takes into account the dynamics of the data set, as the AWS Lambda function also works with many other AWS streaming services. There are three main tasks that the software product solves: prevention and detection of fraud in payment systems, rapid fraud detection (counts in minutes), integration of the software product into the business where payment systems and services are used (for example, payment integration services in financial institutions, online stores, logistics companies, insurance policies, trading platforms, etc.). It is determined that the implementation of an automated system should be considered as a project. The principles of project implementation are offered. It is established that for the rational implementation of the project it is necessary to develop a specific methodology for the implementation of the software product for fraud detection in payment systems of business institutions.

Keywords: Fraud detection; machine learning; automated system; cloud computing; big data; data analysis

For citation: **Khlevna Iu. L., Koval B. S. Development of the Automated Fraud Detection System Concept in Payment Systems. *Applied Aspects of Information Technology*. 2021; Vol.4 No.1: 37–46. DOI: 10.15276/aait.01.2021.3**

INTRODUCTION

The digital transformation of society contributes to the autonomy of customer transactions. Visits to financial institutions are becoming less frequent, and payment systems and services are in increasing demand.

This is facilitated by the growing number of online payments, services for the integration of such payments in financial institutions, online stores, logistics companies, insurance policies, trading platforms, etc. This is due to the ease of use, high speed of financial transactions, simplicity, transparency, control over payments. But, in addition to the advantages of modern payment systems and services, there is a risk – not maintaining the integrity of transactions. Businesses and consumers of goods and services are increasingly faced with such risks. Such risks can be identified as the risk of fraud. The consequence is that consumers do not receive the ordered goods or services, lose money from their accounts. From the business point of view, this is reflected in financial losses, a decrease in customer loyalty, which leads to a complete loss of customers.

In Ukraine in 2020, losses from business fraud amounted to more than UAH 1 billion. Moreover, Ukraine is almost 50 % ahead of the United States in the percentage of fraudulent transactions (10,000 transactions), and this gap is only widening, indicating that not only the industry as a whole needs new solution, but they are especially needed in Ukraine. To prevent this, we need to transform approaches and tools for monitoring, detecting and controlling illegal actions in payment services. Without a doubt, the best way to fight fraud is to prevent it. Therefore, it is advisable to develop scientific and practical approaches to prevent fraudulent transactions.

LITERATURE REVIEW

Using the data [1] such fraud mechanisms have been revealed: social engineering; card-to-card transfers; transfers via online banking; interception of access to mobile banking; counterfeit mobile banking; purchases using Apple Pay and Google Pay; embezzlement via SMS-banking. It has been established that the main type of fraud in the banking sector is payment card fraud. The paper presents some methods of combating fraud and establishes the advantage of using modern technologies, which are based on models and methods of fraud detection. The main essence of the works [2-3], [4-5] is the classification of models of fraudulent operations by different methods. It is advisable to use this approach for fraud detection methods that have been observed previously. The paper [6] forms the approach, according to which a transaction is marked as fraudulent if it deviates from the usual customer behavior. This is based on the assumption that attackers will behave very differently than the account owner. The approach to risk management of fraud with payment systems, which involves a combination of the presented approaches, defined in the works [7-8]. Given the above, it is advisable to first develop and define a model of user behavior, and then detect fraud. Various methods and algorithms can be used to solve this problem. It is worth noting the study presented in [9] – the lack of an effective and accurate algorithm for fraud, which would be the standard for all financial transactions. Each technique has its advantages and disadvantages. In addition, approaches to fraud are dynamic and require constant revision of forecasts, and this is due to the fact that each business in which possible fraudulent schemes are unique and must rely on its own corporate system. An example of the application of unified models of methods under the conditions of specific institutions is presented in the paper [10]. From the standpoint of the application of algorithms for detecting fraudulent transactions in specific businesses, it is appropriate to apply a set of systematic methods of forecasting, detection and control of fraudulent transactions in financial systems, which in [11] were called the fraud detection technologies. Models, methods and algorithms of machine learning are the basis of such technology. The disadvantage of this work is that it does not present the adaptation of the developed model into a software product. However, the market presents a large number of automated systems aimed at preventing fraud, which are called anti-fraud systems [13]. The literature is dominated by information about comprehensive systems for detecting bank fraud. At the heart of such systems are analytical platforms that allow you to implement logic in individual segments. Typically, such systems are used in the banking sector. The examples of such systems are: ARIC White Label by Featurespace, FICO Application Fraud Manager by FICO, FRAUD-Analysis by BSS, IBM Safer Payments by IBM, Fraud and Security Intelligence (SAS FSI) [13-14].

The paper [15-16] presents the principles of operation of systems aimed at identifying instruments of banking fraud. Examples of such systems are: Digital Banking Fraud Detection, WebSafe, IBM Trusteer Rapport, ThreatMetrix, Group-IB Secure Bank, etc.

There are highly specialized systems for detecting signs of bank fraud such as FPS.Bio, SmartTracker.FRAUD.

As well, there are mixed systems for counteracting bank fraud: RSA Adaptive Authentication and Transaction Monitoring, BI.ZONE Cloud Fraud Prevention.

The use of such systems is usually associated with additional costs. In addition, the experience of using ready-made software products shows that such products are not aimed at the concept of detecting local business fraud based on specific available data for an individual company. The implementation of an automated fraud detection system is much broader than the choice of system, and should take into account the range of tasks from the implementation of ideology among employees, formalization of procedures for collecting and storing information to changes in organizational structure and distribution of team roles. This is to some extent reflected in the work [17]. But in the work, there is no description of the automated system. The specialized automated system does not aim to compete with the presented ones, but, on the contrary, will complement their functions.

FORMULATION OF THE PROBLEM

The problem that this work tries to solve is that although there are already built models and algorithms of machine learning, which allow to solve the problem of fraud detection in payment systems, however, in today's world and in modern conditions (given the large data flows , high load, requirements for optimization and performance of the system) it is not only necessary to build a model as, but also to properly implement it in the application environment, so that the resulting software product meets all the requirements of the modern world. That is, the problem of detecting fraud in payment systems is not only to build the algorithmic core, which, based on input data, can isolate fraud, but also to build a reliable, durable automated system that can manage in real time, under high load, data flows and efficiently operate the algorithmic core (previously implemented models) of the system. Such a system should be aimed at the specific conditions of the individual business and is of both scientific and practical interest.

THE AIM OF THE STUDY

Creation of an automated system that is able to analyze the incoming data flow (transactions) in real time and classify them into 2 classes: regular or fraudulent. Propose principles that will take into account the corporate characteristics of companies in detecting fraudulent transactions.

In accordance with the set goal the following research tasks are formed:

– develop the life cycle of the built software product;

– identify technical problems in the development of an automated system and suggest their solutions;

– evaluate the implementation of the developed automated system in business.

The result will be the presence of a prototype of an automated system, which will indicate its architecture, software infrastructure, interfaces, etc.

RESEARCH RESULTS

The identification and configuration of the infrastructure required to build an automated fraud detection system in payment systems. The proliferation and growth of automated systems, the transition from spontaneous automation to the planned development of corporate IT systems, the use of design and business-oriented technologies have created the preconditions for the detection of fraudulent transactions.

It is established that the development of automated technology to prevent fraudulent transactions is accompanied by difficulties associated with:

– the model choosing;

– deployment of the model in the form of automated technology;

– introduction of automated technology in the practice of using business institutions.

CHOICE OF MODEL

In solving this problem, the authors rely on their own research, which is presented in the paper [12].

The following transaction attributes were used to develop the model:

step – displays the unit of time in reality. The transactions in the dataset were completed within 743 hours. That is, “1” – the first hour of observation, “743” – 743rd hour of observation;

type – type of transaction (cash replenishment, cash withdrawal, transfer of funds to the account, payment for goods or services, money transfer);

sum – transaction sum;

nameOrig – the client who initiated the transaction;

oldBalanceOrig – the client's initial balance before the transaction;

newBalanceOrig – customer balance after the operation;

nameDest – identifier (identifier) of the recipient of the transaction;

oldBalanceDest – the initial balance of the recipient;

newBalanceDest – the balance of the recipient after the operation;

isFraud – indicates if the transaction is a fraud (1) or not a fraud (0).

Thus, an analysis was made of a set of banking operations performed by individuals independently - for example, by means of mobile banking, card or terminal – i.e. those operations that were not performed with the help of a bank or other controlling body. It should be noted that the models and the automated system must take into account the dynamics of the data set.

DEPLOYING THE MODEL IN THE FORM OF AUTOMATED TECHNOLOGY

It is advisable to implement a system that is built into the overall automated structure of the company. Therefore, it is proposed to build a cloud web service, which will be fully dedicated to the business process of data analysis and interpretation of the result: whether the transaction is suspicious or not. Cloud technologies help businesses significantly accelerate their response to challenges such as scale and availability, and significantly optimize costs. Development and operation specialists create a user-friendly environment between developers and businesses to increase efficiency, shorten the development cycle and bring the product to market faster. This combination allows to achieve significant changes in the approach to the development of cloud technologies, to respond more quickly to the needs of the enterprise, to consistently integrate the acquired knowledge, to significantly reduce the cost of a number of processes: from testing to deployment [18].

The advantages include:

– scalability: delivering rapid growth by increasing resource efficiency and data center capabilities;

– improved productivity: providing flexible infrastructure to accelerate market entry by eliminating isolated processes;

– rapid cost optimization by reducing or eliminating infrastructure resource losses

– reduce time to market: Cloud migration reduces the time spent building IT infrastructure.

The next step was to choose a platform. The Amazon Web Services (AWS) deployment solution has been found to be the most complete and widely accepted cloud platform in the world, offering more than 200 full-featured data center services worldwide. Millions of customers – including dynamic startups, major businesses and leading government agencies – use AWS to reduce costs, become more flexible and innovate faster [19].

The AWS platform was chosen from the standpoint of assessing its benefits, particularly:

– ease of use – the AWS platform allows you to quickly and securely host both existing and new applications based on the SaaS model. You can use the AWS management console or the Web Services API with detailed documentation to work with the AWS application hosting platform;

– flexibility – AWS allows you to select the operating system, programming language, Internet application platform, database and other necessary services. That is, this platform provides a virtual environment for downloading the software needed to detect fraud. This simplifies the process of migrating the necessary applications and preserves the ability to create new solutions;

– cost-effectiveness – payment is made only for computing power, storage capacity and other resources used without long-term contracts or prior commitments;

– reliability – this platform is the virtual basis of the multibillion-dollar Internet business Amazon.com, the quality of which is confirmed by the practice of use;

– scalability and high performance - AWS tools such as Auto Scaling and Elastic Load Balancing provide scalability. Thanks to Amazon's extensive infrastructure, you have access to computing and storage resources just when you need them.

– security – AWS takes an integrated approach to security and infrastructure strengthening, including physical, operational, and software tools.

Implementation of the automated fraud detection system using cloud technologies.

The concept of implementation of an automated automated fraud detection system (Payment Transactions Fraud Detection – PTFD) in payment systems with the help of AWS platform is next. The solution is to deploy a machine learning model (ML) and an example of a transaction data set to teach the model to recognize fraud patterns [20]. Previously implemented models can learn independently, which will allow them to adapt to new, unknown patterns and patterns. It is appropriate to use this solution to automate the detection of potentially fraudulent activity and to send this activity for verification.

The PTFD system allows you to run automated transaction processing on the example of a data set or on your own data set. The diagram (Fig. 1) shows the deployment architecture. This solution includes the AWS CloudFormation template, which deploys an example of a set of credit card transactions contained in the Amazon Simple Storage Service Recycle Bin (can be replaced with any transaction data set), and an instance of Amazon SageMaker, which trains a controlled and unmanaged learning model. Data set and deploys two endpoints. Based on the application data, a continuous stream of transaction classification requests is generated. The generated queries run the AWS Lambda function, which processes transactions from a sample dataset

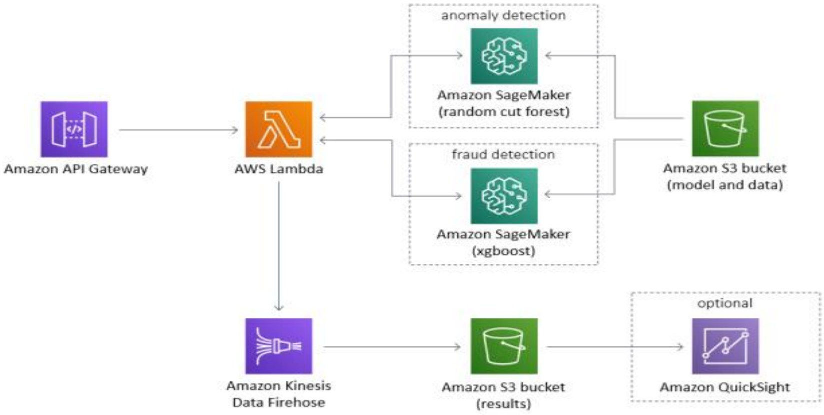
anomaly detection
Amazon SageMaker (random cut forest)
Amazon API Gateway
AWS Lambda
fraud detection
Amazon SageMaker (xgboost)
Amazon S3 bucket (model and data)
optional
Amazon Kinesis Data Firehose
Amazon S3 bucket (results)
Amazon QuickSight

Fig. 1. **Basic architecture of the automated fraud detection system in payment systems (PTFD) based on [21]**

***Source*: [21]**

and calls two Amazon SageMaker endpoints. Endpoints assign an anomaly estimate and predict whether these transactions are fraudulent based on trained ML models. Amazon Kinesis Data delivers processed transactions to another segment of Amazon S3 for storage. Once you've uploaded transactions to Amazon S3, you can use analytics tools and services, including Amazon QuickSight, to visualize, report, query, and analyze in more detail [22].

Amazon Fraud Detector can perform low-delay fraud predictions, allowing the fraud detection system to dynamically adjust customer interactions in real-time fraud detection models. But suppose if you want to generate fraud predictions for a series of events after the fact of the fraud itself; you may not need a low-delay response and you need to evaluate events on an hourly or daily schedule. How to do it with Amazon Fraud Detector?

One approach is to use the Amazon S3 event message to run a lambda function that handles the CSV event file stored in Amazon S3 when the file is loaded into the S3 input segment. The function runs each event via Amazon Fraud Detector to generate predictions using a detector (ML model and rules) and loads the prediction results into the original S3 segment. The following diagram (Fig. 2) illustrates this architecture.

You can also strengthen the system by using Amazon A2I, a machine learning service that simplifies the creation of workflows using the machine learning models needed for human validation. Amazon A2I provides the ability to review developers, eliminating undifferentiated hard work associated with creating review systems performed by people, or managing a large number of reviewers. The high-level solution is summarized in the following architecture [23].

The workflow consists of the following stages (Fig. 3.):

1. The client program sends information to the Amazon Fraud Detector endpoint.

2. Amazon Fraud Detector predicts a risk assessment (ranging from 0 to 1,000) for input using a historical learning machine learning model. A score of 0 means that there is no risk of fraud, and a score of 1,000 indicates that the risk of fraud is maximum.

3. If the risk assessment for a particular forecast falls below a predetermined threshold, no further action is taken.

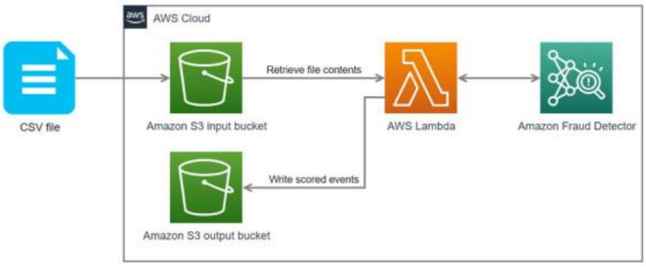

Fig. 2. **Architecture of the automated fraud detection system with start of the classifier with an arbitrary interval [21]**

***Source*: [21]**

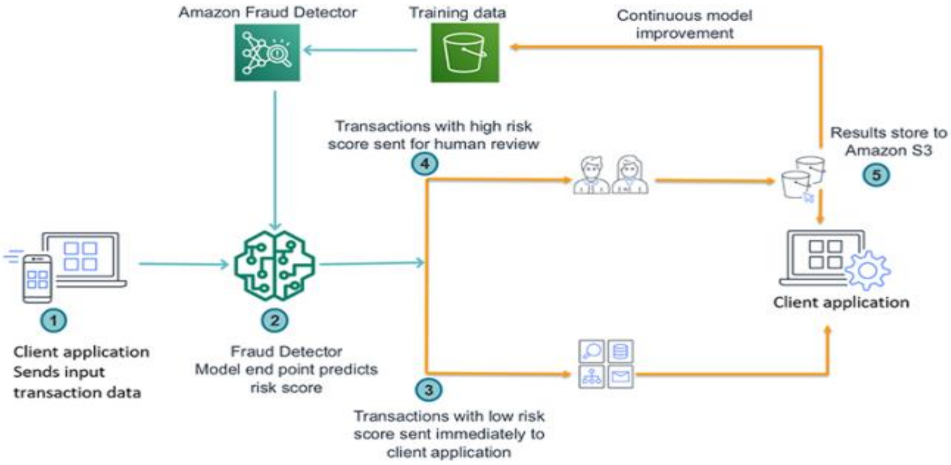
Amazon Fraud Detector
Training data
Continuous model improvement
Transactions with high risk score sent for human review
4
Results store to Amazon S3
5
Client application
1
Client application Sends input transaction data
2
Fraud Detector Model end point predicts risk score
3
Transactions with low risk score sent immediately to client application

Fig. 3. **Real-time fraud detection automated system architecture and integration with client applications [21]**

***Source*: [21]**

4. If the risk assessment exceeds a predetermined threshold (for example, 900 points), the Amazon A2I cycle starts automatically and sends predictions for human verification to the Amazon A2I. Employees of the company can be private personnel. They open the Amazon A2I interface, review the case and make a decision (approve, reject or send it for further verification).

5. The result of approving or rejecting a private workforce is stored in the Amazon Simple Storage Service (Amazon S3). With Amazon S3 it can be sent directly to the client program.

The following steps are required to configure the solution:

1. Training and deployment of the model in Amazon Fraud Detector using historical data.

2. Configure the Amazon A2I cycle for staff using Amazon Fraud Detector.

3. Using the model to predict the risk assessment for given new input data.

4. Customize Amazon A2I workflow and cycles.

Also, to complete the process, consider a solution to detect fraud (anomalies) using the services Amazon DynamoDB Streams and Amazon SageMaker, which will complement the previous implementation and work consistently with it [24].

This solution has the following advantages:

– make better use of available resources to detect anomalies. For example, if you use Amazon DynamoDB streams for disaster recovery (DR) or for other purposes, you can use the data in that stream to detect anomalies. In addition, the backup storage is usually low. Low awareness data can be used for training data.

– automatic retraining of the model with new data on a regular basis, without user intervention.

– simplify the use of the built-in algorithm Amazon SageMaker Random Cut Forest. Amazon SageMaker offers flexible distributed learning options that adapt to specific workflows in a secure and scalable environment.

The stages by which data passes through the architecture (Fig. 4.) are as follows:

1. The DynamoDB source captures changes and saves them in the DynamoDB stream.

2. AWS Glue's task is to regularly retrieve data from the DynamoDB target table and perform training with Amazon SageMaker to create or update model artifacts on Amazon S3.

3. AWS Glue also uses an updated model on the Amazon SageMaker endpoint to detect anomalies in real time based on the Random Forest classifier.

4. The AWS Lambda function analyzes data from the DynamoDB stream and calls the Amazon SageMaker endpoint to draw conclusions.

5. The Lambda function warns user programs after anomalies are detected.

The fraud detection system will look like the final one, after combining all the previous subsystems (Fig. 5).

Thus, 2 artifacts will be transferred to the entrance to the system under development:

– implemented an algorithmic model for detecting fraud (its code), which will be static throughout the life cycle of a single implementation.

– an input set of transaction data that will be dynamic and will change and adapt to the current situation.

In general, the initialization and operation of the system will be implemented in 3 steps: Construction, Training and Placement. After all these 3 steps have been successfully completed, an API access point will be created, with which you can communicate with the implemented automated system.

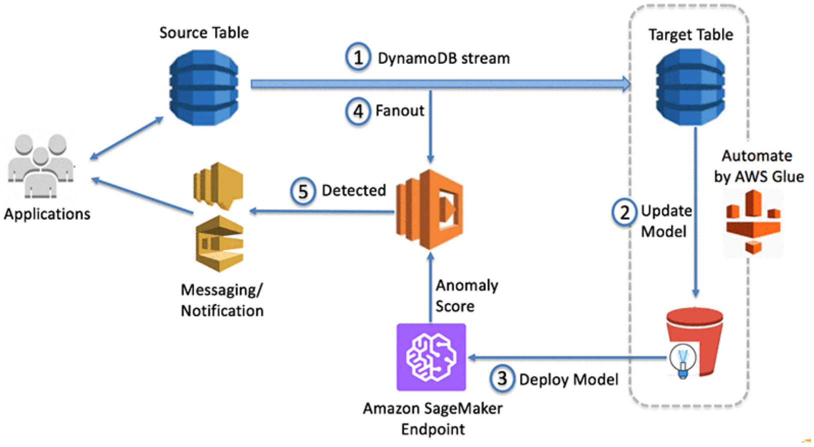

Fig. 4. **Architecture for detecting anomalies in transaction data flows using the implemented automated system [21]**

***Source*: [21]**

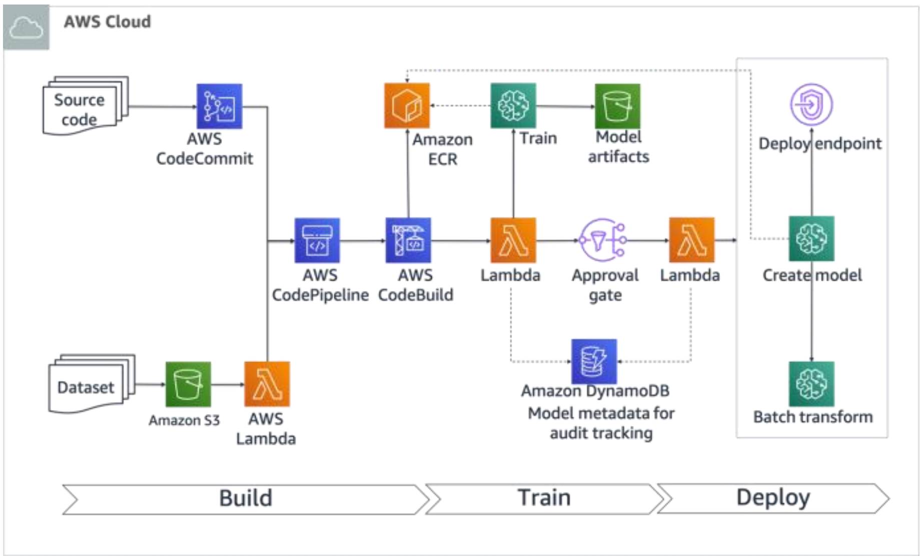

Fig. 5. **Architecture of the full cycle automated fraud detection system [21]**

***Source*: [21]**

As a result, we get a software product that solves the problem:

1. Prevention and detection of fraud in payment systems, because a fully managed solution based on machine learning, which is used to detect fraud. It includes all the tools needed to create, deploy, and manage fraud detection models. In just a few clicks, you can get analytics data that will increase the efficiency of the model through the use of business rules. These rules allow you to control the operation of the model, as well as deploy the results of its work in the form of predictive user-friendly APIs.

2. Detection of fraud in minutes. The system automates the complex stages of creating machine learning models to detect fraud. Any action, from data validation to model deployment, can be performed without machine learning knowledge and programming skills. This allows you to get machine-learning fraud detection models that can be implemented in minutes, not months.

3. Satisfaction of any business needs, because it uses a one-of-a-kind machine learning product that contains patterns of fraudulent actions obtained on the basis of analysis of the data provided. This allows you to create unique fraud detection system settings, optimized for specific business scenarios. This approach provides very high recognition accuracy, reducing the number of false positives.

APPLICATION OF THE AUTOMATED FRAUD DETECTION TECHNOLOGY INTO THE PRACTICE OF BUSINESS INSTITUTIONS

The introduction of an automated system should be considered as a project.

When implementing the project of implementing an automated fraud detection system in payment services, it is recommended to operate with the following principles:

– the operation of the automated fraud detection system must be documented in the business organization;

– systematic assessment of fraud risks and determining the effectiveness of automated technology;

– the automated system should improve fraud detection algorithms;

– investigation of fraudulent transactions.

The costs of the project of implementation of the automated fraud detection system can be estimated through the costs of organizational, technical and methodological indicators:

$$x_m^- = S_m^d + S_m^r + S_m^k,$$

x_m^- – estimation of total costs for the project of implementation of the automated system of fraud detection;

S_m^d – organizational costs for the project of implementation of the automated system of fraud detection;

S_m^r – technical costs for the creation of an automated fraud detection system and a project for its implementation;

S_m^k – methodological costs for the project of implementation of an automated fraud detection system.

Organizational costs are associated with the formation of the organizational structure of the project [25]. The introduction of the developed automated system is appropriate in assessing the technological maturity of the business. It is proposed to use research as such an assessment [26]. Such an assessment is needed because a number of organizational measures are required for a systematic fraud detection process. Such measures are proposed to be implemented in terms of automated business security strategy (development and implementation of strategic vision documents and priorities in the formation of business security policy, corporate security standards, monitoring the implementation of business security policy strategy, automated product promotion strategy, etc.).

Technical costs are costs that are associated with the production costs of software development, as well as with the monitoring and control of the operation of the fraud detection information system.

Methodological costs are related to the development of the automated system development methodology and the implementation project methodology.

Summarizing the above, it can be argued that the implementation is based on the development of a specific methodology for implementing a system for detecting fraud in payment services in financial institutions [27].

CONCLUSIONS

The automated system for detecting fraud in payment systems has been implemented: its architecture, principles and models of operation have been described, and the infrastructure has been set. The paper demonstrates the detection of online fraud using Amazon Fraud Detector and the configuration of human fraud detection workflows using a customizable Amazon A2I task type to verify and confirm high-risk predictions. There is also an example of how to create an anomaly detection system on Amazon DynamoDB streams using Amazon SageMaker, AWS Glue and AWS Lambda. In addition, it is possible to adapt this example to a specific use case, as AWS Glue is very flexible based on the user's script and allows you to add new data sources. Other types of data sources and streams can be used in this architecture, as the AWS Lambda feature also works with many other AWS streaming services.

It is proposed to consider the process of implementing an automated system in business as a project. It is established that for the rational implementation of the project it is necessary to develop a specific methodology for implementing a system for detecting fraud in payment services in financial institutions, which is a prospect for further research.

REFERENCES

1. Dubina, M. V., Sadchikova, I. V. & Seredyuk, I. O. “Conceptual approaches to increasing the level of security of the banking payment environment of Ukraine” (in Ukrainian). Available from: https://www.business-inform.net/export_pdf/business-inform-2020-3_0-pages-349_359.pdf – [Accessed: Jan, 2021].

2. Lebichot, B. & Le Borgne, Y.-A. “Deep-Learning Domain Adaptation Techniques for Credit Cards Fraud Detection”. In: Oneto, L., Navarin, N., Sperduti, A., Anguita, D. (eds.) Recent Advances in Big Data and Deep Learning. *Publ. Springer.* New York: 2019. p. 78–88.

3. Caelen, O. & Smirnov, E. N. “Improving Card Fraud Detection through Suspicious Pattern Discovery”. In: Benferhat, S., Tabia, K., Ali, M. (eds.) *Advances in Artificial Intelligence: From Theory to Practice. Publ. Springer.* New York: 2017. p. 181–190.

4. Pozzolo, A. D., Caelen, O., Bontempi, G. & Johnson, R. A. “Calibrating Probability with Undersampling for Unbalanced Classification”. *Paper presented at the 2015 IEEE Symposium Series on Computational Intelligence.* Cape Town: South Africa. 7-10 December 2015.

5. Lebichot, B., Le Borgne, Y. A., He-Guelton, L., Oblé, F. & Bontempi, G. “Deep-Learning Domain Adaptation Techniques for Credit Cards Fraud Detection”. In: Oneto L., Navarin N., Sperduti A., Anguita D. (eds). Recent Advances in Big Data and Deep Learning. *INNSBDDL 2019. Proceedings of the International Neural Networks Society. Publ. Springer.* 2020; Vol. 1. Cham: DOI: https://doi-org-443.webvpn.jnu.edu.cn/10.1007/978-3-030-16841-4_8.

6. Sorournejad, S. Z. Zojaji, R. E. & Atani Hassan Amir. “Monadjemi Fraud Detection Techniques”. Data and Technique Oriented Perspective. Cornel University Library. 2016. – Available from: https://arxiv.org/ftp/arxiv/papers/1611/1611.06439.pdf (date when it was last valid – 20.10.2020).

7. Kuznietsova, N. V. “Analysis and forecasting the risks of credit card fraud”. *Informatics and Mathematical Methods in Simulation* (in Ukrainian). 2018; Vol. 8 No. 1: 16–25.

8. Kuznietsova, N. V. “Scoring Technology for Risk Assessment of Fraud in Banking”. *Selected Papers of the XVI International Scientific and Practical Conference “Information Technologies and Security” (ITS 2016)* (in Ukrainian). 2016. p.54–61.

9. Delamaire, Linda, Abdou, Hussein & Pointon, John. “Credit card fraud and detection techniques: a review”. *Banks and Bank Systems*. 2009; Vol. 4 Issue 2.

10. Teslia, I., Yehorchenkov, O., Khlevna, I. & Khlevnyi, A. “Development concept and method of formation of specific project management methodologies”. *Eastern-European Journal of Enterprise Technologies* (in Ukrainian). 2018; No.5/3(95): 6–16.

11. Khlevna, I., Koval, B. “Fraud detection technology in payment systems” *Information Technology and Interactions (Satellite): Conference Proceedings*. December 04, 2020, Kyiv, Ukraine. Taras Shevchenko National University of Kyiv and [etc]; Vitaliy Snytyuk (Editor). *Publ. Stylos* (in Ukrainian). Kyiv: 2020. p.150–153.

12. Sapozhnikova, M. U., Nikonov, A. V., Vulfin, A. M., Gayanova, M. M., Mironov K. V. & Kurennov, D. V. “Anti-fraud system on the basis of data mining technologies”. *2017 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*. Bilbao: Spain. 2017. p.243–248. DOI: 10.1109/ISSPIT.2017.8388649.

13. Lopez-Rojas, E. A. & Axelsson, S. “A review of computer simulation for fraud detection research in financial datasets”. *Future Technologies Conference (FTC)*. 2016. p.932–935.

14. Fang, W., Li, X., Zhou, P., Yan, J., Jiang, D. & Zhou, T. “Deep Learning Anti-Fraud Model for Internet Loan: Where We Are Going”." In *IEEE Access*. 2021; Vol.9: 9777–9784. DOI: 10.1109/ACCESS.2021.3051079.

15. Wang Hongbin. “Research and Application of web Log Mining Technology Based on Distributed Computing Platform [D]”. (2015). Shandong University Jinan. 2020; Vol.3 No.3: 133–144. DOI: 10.15276/aait.03.2020.2.

16. Sheremet, O. I., Korobov, O. Ye., Sadovoi, O. V., Sokhina, Yu. V. “Intelligent System Based on a Convolutional Neural Network for Identifying People without Breathing Masks”. *Applied Aspects of Information Technology*. *Publ. Science i Technical*. Odesa: Ukraine. 2020; Vol.3 No.3: 133–144. DOI: 10.15276/aait.03.2020.2.

17. Halbouni, S. S., Obeid, N. & Garbou, A. “Corporate governance and information technology in fraud prevention and detection: Evidence from the UAE”. *Managerial Auditing Journal*. 2016; Vol. 31 No. 6/7: 589–628. DOI: https://doi.org/10.1108/MAJ-02-2015-1163.

18. “Cloud computing”. SoftServe. 2021. – Available from: https://www.softserveinc.com/uk-ua/services/cloud-devops. – [Accessed: Jan, 2021].

19. “Overview of Amazon Web Services”. 2021. – Available from: https://d1.awsstatic.com/ whitepapers/aws-overview.pdf. – [Accessed: Jan, 2021].

20. “Cloud Computing Solutions Architect: A Hands-On Approach”. A Competency-based Textbook for Universities and a Guide for AWS Cloud Certification and Beyond by Arshdeep Bahga, Vijay Madisetti. VPT. 2019. 346 p.

21. “AWS Documentation”. 2021. – Available from: https://docs.aws.amazon.com/ index.html?nc2=h_mo. – [Accessed: Jan, 2021].

22. “AWS Certified Cloud Practitioner Study Guide: CLF-C01 Exam”. 1st Edition by Ben Piper, David Clinton.

23. “Architecting Cloud Computing Solutions: Build cloud strategies that align technology and economics while effectively managing risk”, by Kevin L. Jackson, Scott Goessling, May 30, 2018.

24. “Designing Data-Intensive Applications: The Big Ideas Behind Reliable, Scalable, and Maintainable Systems”, by Martin Kleppmann. April 18. 2017.

25. Mezentseva, O. O. & Kolomiiets, A. S. “Optimization of Analysis and Minimization of Information Losses in Text Mining”. *Herald of Advanced Information Technology. Publ. Science i Technical*. Odesa: Ukraine. 2020; Vol.3 No.1: 373–382. DOI:10.15276/hait.01.2020.4.

26. Bushuev, S.D. & Bushueva, N.S. “Development of technological maturity in project management”. *Project management and production development. Collection of scientific works. Ed. В.А.Рач.* (in Ukrainian). 2003; No. 2 (7): 5–12.

27. Teslia, I. M., Khlevna, I. L., Yehorchenkov, O. V. & Yehorchenkova, N. I. “Organizational bases of implementation of Specified project management”. Methodologies. Sciences of Europe. *Technical sciences* (in Ukrainian). 2018; Vol. 1 No. 34: 12–18.

Conflicts of Interest: the authors declare no conflict of interest

Received 02.02.2021
Received after revision 04.03.2021
Accepted 12.03.2021

DOI: 10.15276/aait.01.2021.3
UDC 004.89

РОЗРОБКА КОНЦЕПЦІЇ СТВОРЕННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ ВИЯВЛЕННЯ ШАХРАЙСТВА В ПЛАТІЖНИХ СИСТЕМАХ

Юлія Леонідівна Хлевна[1)]
ORCID: http://orcid.org/0000-0002-1807-8450, yuliya.khlevna@gmail.com
Богдан Сергійович Коваль[1)]
ORCID: http://orcid.org/0000-0002-3757-0221, bohkoval@gmail.com
[1)] Київський національний університет імені Тараса Шевченка, вул. Володимирська, 60, Київ, 01033, Україна

ABSTRACT

У роботі представлено попит поширення платіжних систем. Таке поширення пов’язане із розвитком технологій. Виокремлено відкрите питання застосування платіжних систем – шахрайство. Встановлено, що не існує ефективного алгоритму, який би був стандартом для всіх фінансових установ при виявленні, запобіганні шахрайства. Це пов’язано із тим, що підходи до шахрайства є динамічними та вимагають постійної переробки прогнозів. Визначено перспективи розвитку науково-практичних підходів попередження шахрайських операцій при здійсненні транзакцій. Встановлено, що машинне навчання є доречним у рішенні задач виявлення шахрайства у платіжних системах. Але виявлення шахрайства в платіжних системах полягає не тільки в побудові самого алгоритмічного ядра, але й у побудові надійної автоматизованої системи, яка в режимі реального часу, за умови високого навантаження, здатна керувати потоками даних та ефективно оперувати алгоритмічним ядром системи. У роботі описано архітектуру, принципи та моделі функціонування, інфраструктуру автоматизованої системи виявлення шахрайства в платіжних системах. Визначено доцільність застосування хмарного веб-сервісу. Обгрунтовано розгортання моделі у вигляді автоматизованої технології базі платформи Amazon Web Services. Основою автоматизованої системи виявлення онлайн-шахрайства є Amazon Fraud Detector і налаштування робочих процесів перевірки шахрайства в платіжних системах за допомогою настроюваного типу завдання Amazon A2I для перевірки і підтвердження прогнозів з високим ризиком. Наведено приклад створення системи виявлення аномалій на потоках Amazon DynamoDB за допомогою Amazon SageMaker, AWS Glue та AWS Lambd. Автоматизована система враховує динамічність набору даних, оскільки функція AWS Lambda також працює з багатьма іншими потоковими службами AWS. Виокремлено основні три завдання, які вирішує програмний продукт: запобігання та виявлення шахрайства в платіжних системах, виявлення шахрайства за лічені хвилини, інтеграція програмного продукту у бізнес, де використовуються платіжні системи та сервіси (наприклад, сервіси інтеграції платежів у фінансових установах, інтернет-магазинах, логістичних компаніях, страхових полісах, торгових майданчиках, тощо). Визначено, що впровадження автоматизованої системи доречно розглядати як проєкт. Запропоновано принципи впровадження проєкту. Встановлено, що для раціонального впровадження проєкту потрібно розробити конкретизовану методології впровадження програмного продукту виявлення шахрайства у платіжних системах бізнесових установ.

Ключові слова: виявлення шахрайства; машинне навчання; автоматизована система; хмарні обчислення; великі дані; обробка даних

ABOUT THE AUTHORS

Iuliia L. Khlevna, Doctor of Technical Sciences, Associate Professor of the Department of Technologies Management, Taras Shevchenko National University of Kyiv, Volodymyrska str., 60, Kyiv, 01033, Ukraine
ORCID: http://orcid.org/0000-0002-1807-8450; yuliya.khlevna@gmail.com
Research field: Project Management Methodology; Information Technology in Management; Intelligent Information Technologies; Data Science

Юлія Леонідівна Хлевна, д-р техніч. наук, доцент каф. Технології управління Київського національного ун-ту імені Тараса Шевченка, вул. Володимирська, 60, Київ, 01033, Україна

Bohdan S. Koval, Master's Degree Student Department of Technology Management, Taras Shevchenko National University of Kyiv, Volodymyrska str., 60, Kyiv, 01033, Ukraine
ORCID: http://orcid.org/0000-0002-3757-0221, e-mail: bohkoval@gmail.com,
Research field: Information Technology in Management; Intelligent Information Technologies; Data Science; Machine Learning

Богдан Сергійович Коваль, студент магістратури кафедри Технології управління Київського національного ун-ту імені Тараса Шевченка, вул. Володимирська, 60, Київ, 01033, Україна
ORCID: http://orcid.org/0000-0002-3757-0221; bohkoval@gmail.com