IMPROVING ACCESS RESTRICTIONS IN COMMERCIAL BANKS INFORMATION SYSTEMS BASED ON RISK MODEL AND SMART-Q ALGORITHM

Kobiljanov Sh. N.
Independent researcher at Tashkent University of
Information Technologies named after Muhammad al-Khwarizmi

Abstract

This in the article commerce banks information in systems use management and restriction processes modern at risk-based approaches through improvement issues illuminated. Research within information in systems use management risk model in the process based on organization done protection mechanism exemplary structure shaped and in practice wide being used there is models disadvantages analysis Commercial banks information to systems typical real time in mode performance , high transaction density and information to safety to be placed strict requirements in consideration taken , risks to time dependency and variability into account recipient improved risk model offer Also , based on semantic mapping information only to format to bring directed and via API use restriction in the process information integration SMART-Q algorithm providing working issued . Proposal done approach commerce banks information in systems risks more precisely evaluation , errors fast identification , integration processes simplification and use restriction efficiency increase opportunity gives .

Keywords: Commerce banks , information system , usage management , risk model , real time systems , tail risk, data integration , SMART-Q algorithm , API, semantic mapping.

In the current conditions of rapid development of digital transformation processes, the activities of commercial banks rely on complex and multi-component information systems. Remote banking services, online payments, mobile applications and integration with external financial platforms are leading to a sharp increase in the volume of data exchange in banking information systems. Along with these processes, improving information security, preventing unauthorized access and restricting access mechanisms is becoming one of the important scientific and practical tasks.

Traditional access control models, in particular static rules or purely role-based approaches, often fail to fully account for threats and risks that arise in real time. In the case of commercial banking information systems, risks are dynamic and change over time. Therefore, it is important to assess risks over time, take into account their interaction and identify tail risks.

This article addresses these issues by improving the risk model-based access restriction mechanism and developing the SMART-Q algorithm that provides data integration.

Specific features of access control in information systems of commercial banks

Information systems of commercial banks differ from other types of information systems in a number of specific features. Firstly, these systems operate in real time, and each delay can lead to financial losses. Secondly, highly confidential information is stored and processed in the systems. Thirdly, seamless integration with external and internal systems is required.

Therefore, access management requires not only user identification and authentication, but also real-time risk assessment and appropriate restrictions. The proposed model focuses on these aspects.

A typical structure of a protection mechanism based on a risk model

The protection mechanism, based on the risk model in the information system access management process, consists of several functional layers, each of which performs specific tasks. This structure allows for a comprehensive analysis of the user, resource, and system status.

The main elements of the model structure include:

user behavior monitoring module;

risk assessment and forecasting module;

usage restriction and decision-making module;

security policy and rule base.

The main drawback of many risk models used in practice is their static nature. Such models assess risks at a specific point in time, but do not adequately account for changes in risk levels over time.

Improved model that takes into account risk variability

In this study, the risk model was improved by introducing a cross-risk coefficient into the time-dependent functions, taking into account risk variability. The cross-risk coefficient represents the interrelationship between different risk factors and allows for the assessment of their combined effect.

The improved model considers the risk level as a function of time. This allows for continuous monitoring of the system status in real time and rapid response to a sharp increase in risks. In particular, tail risks are given special attention.

As a result, in the process of restricting the use of commercial banks' information systems:

the time dependence of risks is taken into account;

high-impact risks are identified;

resource utilization is optimized;

A balance is achieved between security and continuity of services.

SMART-Q algorithm and data integration

The effectiveness of the process of restricting access in commercial banks' information systems largely depends on the quality of data integration. Data coming from different sources may be in different formats, which complicates the analysis process.

To solve this problem, the SMART-Q algorithm was developed, which is aimed at bringing data into a single format based on semantic mapping. The algorithm semantically adapts data coming from systems integrated via API and brings it into a single logical model.

The main advantages of the SMART-Q algorithm are:

real-time detection of errors in the information system;

easy and efficient data exchange between integrated systems and resources;

ensuring the completeness, accuracy and reliability of information;

increasing the accuracy of decision-making in the use restriction process.

Combination of risk model and SMART-Q algorithm

The proposed risk model and the SMART-Q algorithm work in harmony with each other. The data integrated and cleaned by the SMART-Q algorithm is transmitted to the risk model. The risk model, in turn, calculates the risk level in real time based on this data and makes decisions on limiting use.

This approach significantly increases the overall efficiency of the process of restricting access to information systems of commercial banks and brings it up to the level of modern requirements for ensuring information security.

The article provides a detailed analysis of the risk-based approach and the SMART-Q algorithm aimed at improving the processes of controlling and restricting access in information systems of commercial banks. An improved risk model that takes into account the time dependence and variability of risks allows for a more accurate assessment of threats arising in bank information systems. The SMART-Q algorithm, developed based on semantic mapping, simplifies data integration, improves the quality of real-time error detection and decision-making. The research results show that the practical implementation of the proposed approach in information systems of commercial banks will serve to increase the efficiency of the access restriction process.

References

1 ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

2 ISO/IEC 27005:2022. Information security risk management.

3 Hu V.C., Ferraiolo D., Kuhn D.R. Guide to Attribute Based Access Control (ABAC). NIST SP 800-162, 2020.

4 NIST SP 800-53 Rev.5. Security and Privacy Controls for Information Systems and Organizations, 2020.

5 Shafiq M., Tian Z., Bashir A.K. Security and Privacy of Banking Systems: Access Control Perspectives. Future Generation Computer Systems, 2021.
6 Behl A., Behl K. Cyberwar and Information Security Risks in Financial Institutions. Oxford University Press, 2021.
7 Kumar R., Mishra P. Real-Time Risk-Aware Access Control Models for Financial Systems. IEEE Access, 2022.
8 Alasmary W., Alhaidari F. Data Integration and Risk Management in Banking Information Systems. Journal of Information Security, 2023.