Application of AI Technology in Internet Finance and Analysis of Security Risks

Ou Wang[1], Huan Ye[2], and Runfa Li[3](✉)

[1] Guangzhou Huali Science and Technology Vocational College, Zengcheng, Guangzhou 511325, China
[2] Guangzhou International Economics College, Guangzhou 510540, China
[3] Guangzhou College of Technology and Business, Guangzhou 510850, China
lirunfa@gzgs.edu.cn

Abstract. Internet finance is a new financial market formed by the interaction of traditional financial markets and emerging financial markets. In this article, we will focus on how to use AI technology to analyze security risks. Artificial intelligence (AI) is an intelligent technology that can make decisions based on certain knowledge or rules without human intervention. AI can help us reduce human error. The application of artificial intelligence technology in internet finance is becoming increasingly widespread, including risk control, customer service, intelligent investment advisory, and other fields. Among them, artificial intelligence algorithms can help financial institutions determine whether there are risks based on users' personal information and behavior patterns, improve risk management level, and improve service quality. At the same time, artificial intelligence technology can also provide personalized investment advice to customers, helping them achieve better returns. However, the application of artificial intelligence technology in internet finance also brings some security risks. For example, hackers can exploit algorithmic vulnerabilities, attack artificial intelligence systems, and steal users' personal information and funds. In addition, artificial intelligence systems are susceptible to human manipulation and erroneous indications, resulting in misjudgment and bias. This requires financial institutions to adopt strict security measures, improve their technological level, ensure the safety and privacy of customers, and ensure the sustainable and healthy development of artificial intelligence technology.

Keywords: finance · artificial intelligence · internet · security risk

1 Introduction

Various financial business models such as P2P financing, cash lending, crowdfunding, digital currency, online payment, and online banking have been derived. In the process of operation and operation of Internet financial products based on cash loan mode, various artificial intelligence resources for intelligent data processing and analysis, such as: the risk coefficient that customers can bear, the customer's good credit, the risk of fraudulent loans and bad debts [1].

J. C. Hung et al. (Eds.): FC 2023, LNEE 1132, pp. 354–359, 2024.
https://doi.org/10.1007/978-981-99-9538-7_55

More and more Internet financial enterprises have been applied to risk control management based on AI technology. The use of AI helps to continuously improve the risk control system and establish a lasting risk control system. Compared with traditional risk control technology, AI risk control adds more dimensions and relevance analysis. Traditional risk control judges whether a person has loan qualification, reviews deposits, income, collateral, family conditions, etc., and sets medical access threshold [2]. If it fails to meet the requirements, it cannot apply for loans. AI risk control can find data from other aspects, not only financial data, but also social data, payment data and life service data of borrowers.

These personal data information are highly sensitive and of great value. The security construction of artificial intelligence platform has become the top priority of information security construction and risk management of Internet financial enterprises.

2 Related Work

2.1 Application and Research Status of AI Technology in Internet Finance

At present, the domestic research on AI and Internet finance mainly includes two aspects: the research on Internet financial security risk and regulatory mechanism: Zhang Chenghui (2016) proposed that the Internet financial activities should be targeted according to the exposed problems, the differentiated regulatory and risk control system should be adopted for the Internet financial platform, the cross-sectoral coordination and supervision should be strengthened, and the behavior supervision of formal financial institutions should be strengthened [3], We will intensify efforts to crack down on illegal fund-raising and strengthen risk education for investors. Hou Jianqiang et al. (2016) believed that payment innovation information behavior of traditional finance [4]. The diversification of information sources processing technology have brought new technologies and resources to Internet financial risk management.

Hu Chen (2017), starting from the characteristics of P2B industry, demonstrated the structural path of P2B Internet financial risk by means of questionnaire survey and analysis, and thus proposed seven principles of controllable P2B Internet financial risk. Analyzed the possible impact of AI application, and put forward countermeasures on this basis. Cheng Dongliang (2016) introduced the application status of AI in the financial field, analyzed the risks faced in its development, and based on this, put forward suggestions such as strengthening access control and identity authentication, introducing audit measures and monitoring measures.

At present, there are few documents and materials to discuss the issues of Internet finance in the context of AI. The existing research on the security risks and monitoring mechanism of Internet finance is still based on the past technical standards.

2.2 Concept and Characteristics of Internet Finance

Internet finance, that is, the “Internet plus finance” model. In 2012, Professor Xie Ping first proposed the concept of “Internet finance”. His main report, “Research on Internet Finance Models”, details the definition of Internet finance and its three core parts: payment method, information processing and resource allocation.

The data security capability maturity model was jointly drafted by Alibaba (Beijing) Software Service Co., Ltd., China Information Security Evaluation Center, Tsinghua University, the Institute of Software of the Chinese Academy of Sciences, the National Information Security Engineering and Technology Research Center, Huawei Technologies Co., Ltd., and 3600 Technology Co., Ltd, It is issued by the National Technical Committee for Information Security Standardization (SAC/TC 260).

3 Information Security Risk Analysis and Protection Strategy Research of Internet Financial Enterprises

3.1 Make Full Use of Data Security Capability Maturity Model

The data security Capability Maturity Model is a way to evaluate the organization's data security capabilities, which can help organizations understand their own security capabilities, find weaknesses in security management and improve measures, so as to improve the level of data security assurance. In terms of making full use of the data security Capability Maturity Model, organizations should start from the following points:

Determine the standard model: There are a variety of data security Capability Maturity Model to choose from, and organizations need to choose their own standard models according to the actual situation. For example, organizations can choose a maturity model based on NIST CSF or customize it according to other standards.

Conduct security assessment: Organizations need to evaluate their data security capabilities based on the selected standard model, understand the current status of security capabilities, and identify security vulnerabilities.

Develop an improvement plan: After the evaluation is completed, the organization needs to develop a data security improvement plan, specifying improvement goals and measures.

Implementation of improvement measures: Organizations should gradually improve their safety capabilities in accordance with the established improvement plan, such as strengthening risk assessment and safety awareness training.

Continuous improvement: Organizations need to continuously improve the maturity of data security capabilities through regular security assessments, and further enhance the level of security assurance.

By making full use of the data security Capability Maturity Model, organizations can fully understand their own data security situation, find shortcomings, develop corresponding improvement measures, and constantly improve the level of data security assurance.

Figure 1 above is the data security capability maturity capability building framework. It is designed according to the capability maturity level 3 (fully defined level). Each module is designed to meet the following requirements:

Compliance and business requirements: For any organization, before carrying out the process of data security capacity building, it must be based on the premise of meeting national laws and regulations. It can ensure business development and promote business production through data security construction.

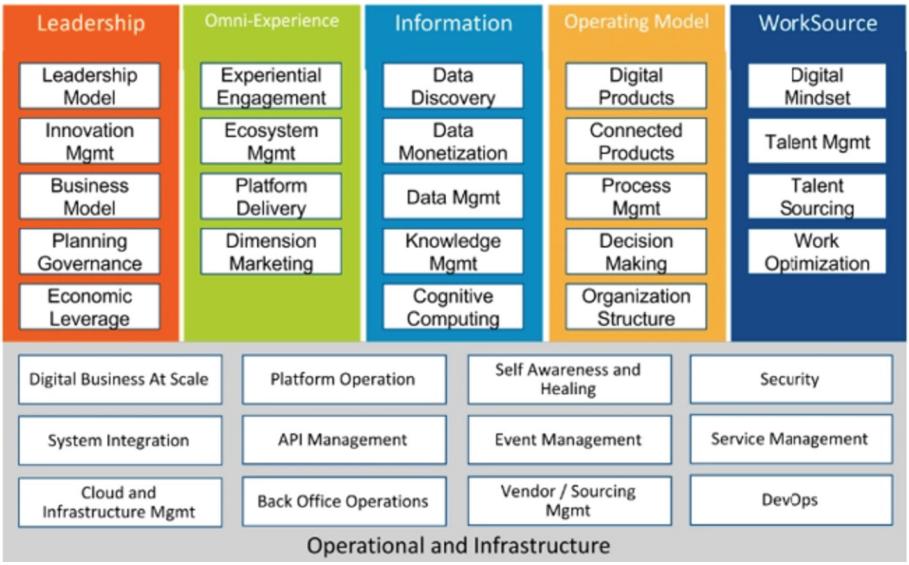

Fig. 1. Data security mature capacity building framework

Organization construction: data security construction can not be completed by one or two people. It needs a special data security organization. The data security organization should be established and its responsibilities should be defined.

System process: establish data security management system and promote its implementation, including data security system charter and management specifications.

Technical tools: technologies and tools supporting the data security system, promoting effective implementation, and security technology platform tools at all stages of the data life cycle.

Personnel capabilities: the capabilities required to ensure data security organization construction, system process, technical tool construction and implementation. The core capabilities include data security management, data security operation, data security technology and other security capabilities.

3.2 Use Machine Learning and Neural Network to Assist Decision-Making and Early Warning

The field of Internet finance is basically a pure data field. AI can serve as an online intelligent financial adviser, provide appropriate financial investment plans for users according to the calculation and analysis results and their personal investment experience, and calculate risks for users for reference. The application of AI in Internet financial decision-making mainly refers to the provision of algorithmic online investment advisory and asset management services for customers, often referred to as intelligent investment advisory.

For example, making full use of cognitive computing, intelligent robot process automation, identity analysis, network analysis, machine learning and other advanced

analysis functions can speed up due diligence and help Internet financial enterprises effectively understand and manage a large number of anti-money laundering alerts generated by the existing transaction monitoring system. Combining the advantages of AI technology, financial institutions can improve the speed and accuracy of customer authentication, collect negative news to understand customer requirements, thus reducing false reports and speeding up the investigation of anti-money laundering alert review. Compared with human work, AI has higher stability and will not be tired, and its analysis and decision-making will not be affected by external factors.

4 Application Structure Research

The application of artificial intelligence technology in internet finance has broad prospects, which can help financial institutions improve their risk control capabilities and customer service quality, and provide intelligent investment advisory and personalized services to customers. However, with the increasingly widespread application of artificial intelligence technology, there are also some security risks, including the exploitation of algorithm vulnerabilities, hacker intrusion into systems to steal customer personal information and funds, artificial intelligence systems being manipulated, and so on.

In order to address these security risks, financial institutions need to take a series of measures. Firstly, strengthen data encryption and identity recognition technologies to enhance data security capabilities; At the same time, organizations should pay attention to the following issues when using the data security Capability Maturity Model:

Model selection: Different standard models have their own advantages and disadvantages for organizations, so when choosing, organizations should consider their own situation comprehensively and customize appropriate models to truly leverage the advantages of the models.

Evaluation object: The organization should clearly define the scope of evaluation objects, such as customer data, financial data, etc. The evaluation scope varies, and the evaluation results also vary. Therefore, all data that needs to be protected should be considered.

Data dynamics: the data security Capability Maturity Model can only reflect the current status of data security at a certain time, and the organization should regularly evaluate it to maintain dynamic monitoring of data security status.

Employee training: Organizations should strengthen employee training, enhance security awareness and skills, enable employees to understand the importance of data security, and enhance their sense of responsibility for data security.

To sum up, the data security Capability Maturity Model is a good tool for evaluating the organization's data security capabilities, which can help organizations fully understand their own data security situation, find and improve weak links, and constantly improve the level of data security assurance. However, attention should be paid to the above issues to ensure that effective implementation methods are followed.

5 Conclusion

When making decisions and implementing artificial intelligence systems, people do not want their actions to violate the basic ethics and moral principles of human society. Therefore, it is necessary to consider this issue at all times during the design and development stages of artificial intelligence systems. Therefore, it is necessary to establish ethical norms and technological research and development norms for artificial intelligence. Researchers of AI systems need to conduct ethical and moral hazard assessments of products to ensure that AI systems will not engage in anti human and anti-social behaviour.

References

1. Khanagar, S.B., Vishwanathaiah, S., Naik, S., et al.: Application and performance of artificial intelligence technology in forensic odontology - a systematic review. Legal Med. (48), 48 (2021)
2. Filipiak, D., Stróyna, M., Wcel, K., et al.: Application of AI and in-memory computing for extracting vessel movement patterns from historical data. In: 14th NATO Operations Research and Analysis (OR&A) Conference: Emerging and Disruptive Technology: Meeting Proceedings, North Atlantic Treaty Organization (2021)
3. Liu, A., Zhang, G., Zou, Q., et al.: New Application of Horizon Flattening Technology with Seismic Data for Exploration and Development in Fula Sub-basin, Muglad Basin, Sudan (2021)
4. Buffon, E., Mendona, F.: Application of RPAs to disaster risk reduction in Brazil: application in the analysis of urban floods. J. Unmanned Veh. Syst. (2021)