International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Check for updates

Machine learning algorithms to prevent fraudulent transactions in real-time

U Somayajulu, A Surender and N Mriganka

Individual Researcher, Pune, Maharashtra, India.

International Journal of Science and Research Archive, 2024, 13(01), 2027–2033

Publication history: Received on 19 August 2024; revised on 02 October 2024; accepted on 04 October 2024

Article DOI: https://doi.org/10.30574/ijsra.2024.13.1.1847

Abstract

In the rapidly evolving landscape of digital finance, the proliferation of online transactions has been accompanied by a significant increase in fraudulent activities. This paper explores the application of machine learning algorithms to detect and prevent fraudulent transactions in real-time, thereby enhancing the security and reliability of financial systems. We investigate various machine learning techniques, including supervised learning models such as Random Forest, Logistic Regression, and Neural Networks, as well as unsupervised methods like anomaly detection. By leveraging these algorithms, we aim to identify patterns and anomalies indicative of fraudulent behavior. Our approach integrates robust preprocessing techniques and real-time data analysis to ensure high accuracy and efficiency. The results demonstrate that machine learning models can significantly reduce the incidence of fraud, providing financial institutions with a powerful tool to safeguard their customers' assets. This study underscores the potential of machine learning to transform fraud detection, offering a scalable and adaptive solution to one of the most pressing challenges in the financial sector

Keywords: Artificial intelligence; Cyber threats; Financial services; Data security; Risk assessment

1. Introduction

Cyber security is a crucial issue in the modern world, as various cyberspaces are used by criminals to conduct cybercrime and cyber threats. To cope with these challenges, the banking and financial industry has adopted artificial intelligence (AI) as a promising technology that can perform various functions associated with human minds, such as reasoning, learning, interacting, creating, perceiving, and problem-solving. AI can also handle large volumes of structured and unstructured data, extract useful patterns and insights, and control individual human behavior, inference methods, and knowledge representation. However, AI also has some limitations and risks, such as ethical, legal, social, and technical aspects. This paper aims to explore the applications and implications of AI in the context of cyber security and cybercrime prevention. It will discuss the various methods and techniques of AI that are used to execute various tasks and solve problems related to cyber security. It will also analyze the benefits and drawbacks of AI in the banking and financial sector, and suggest some ways to improve the performance and reliability of AI systems.

1.1. Cyber security in Banking

Cyber security in banking is a very important topic, as banks are often the target of cyber attacks that aim to steal money, data, or disrupt services. Cyber security in banking covers the technology and protocols for preventing and responding to attacks that target financial institutions' data, networks and digital infrastructure. Some examples of cyber security in banking are:

* Corresponding author: U Somayajulu, A Surender and N Mriganka

- Network security surveillance: This involves continuously scanning a network for signs of dangerous activity, such as malware, unauthorized access, or data breaches. Network security surveillance helps to detect and respond to cyber threats in real time and prevent further damage.
- Software security: This involves protecting the applications that are essential to business operations, such as online banking, mobile banking, or payment systems. Software security ensures that the applications are free from vulnerabilities, bugs, or malicious code that could compromise their functionality or integrity.
- Risk management: This involves identifying, assessing, and mitigating the potential risks that could affect the bank's cyber security posture. Risk management helps to prioritize the most critical assets, systems, and processes, and implement appropriate controls and measures to reduce the likelihood and impact of cyber incidents.
- Cyber resilience: This involves preparing for, responding to, and recovering from cyber attacks that could disrupt the bank's normal operations. Cyber resilience helps to maintain the continuity of service delivery, minimize the damage and losses, and restore the confidence and trust of customers and stakeholders.
- Cyber awareness: This involves educating and training the bank's employees, customers, and partners on the best practices and behaviors for cyber security. Cyber awareness helps to create a culture of cyber security within the bank, and reduce the human errors or negligence that could expose the bank to cyber risks.
- Cyber governance: This involves establishing and enforcing the policies, standards, and regulations for cyber security within the bank. Cyber governance helps to align the cyber security objectives with the business goals, ensure compliance with legal and ethical requirements, and monitor and evaluate the cyber security performance.

Cyber security in banking is a vital aspect of ensuring the safety and prosperity of the financial sector. As cyber threats become more sophisticated and prevalent, banks need to adopt a proactive and holistic approach to cyber security that covers all aspects of prevention, detection, response, and recovery. By doing so, banks can protect their assets, customers, and reputation from cyber attacks.

1.2. Cyber crime and its imapact in banking

Cybercrime is a serious threat to the global economy, especially to the banking and financial sector. According to a survey, cybercrime cost the world $450 billion in 2016, with Asian organizations losing more than $81 billion. Some of the common types of cyber-attacks are denial-of-service attacks, infrastructure attacks, and data breaches (Vieira and Sehgal 2018). Most of the CEOs of the capital market and banks regard cyber security as a challenge to their growth. The financial service organizations face security incidents 300 times more often than other businesses in different industries. Moreover, the financial service industry is the target of 33% of large attacks. Therefore, it is essential to develop some security programs to protect the banking sector from cyber threats. The global banking and financial industry estimates that cyber-attacks cost them around $360 billion per year. In recent years, the financial institutions have been affected by global ransomware attacks. To fight against hackers, many banks are trying to implement artificial intelligence.

1.3. Constraints to use Artitificial Intelligence in banking industry

Data quality and availability: Banks often lack enough and reliable data to train and use AI models effectively. They may need to access external data sources or partner with other entities to enrich their data. They may also face privacy and security issues when handling sensitive customer data.

Regulatory and ethical compliance: Banks need to comply with various regulations and ethical standards when using AI, such as ensuring fairness, transparency, explainability, and accountability. They may need to adopt frameworks and guidelines to ensure that their AI applications are aligned with the law and the expectations of customers, regulators, and society.

Organizational and cultural readiness: Banks need to transform their organizational structures, processes, and cultures to embrace AI and foster innovation. They may need to invest in talent development, change management, and agile ways of working. They may also face resistance from employees who fear being replaced by AI or lack the skills to work with it.

Integration with legacy systems: Banks need to integrate their AI applications with their existing IT systems, which may be outdated, complex, or incompatible. They may need to upgrade their IT infrastructure, adopt cloud-based solutions, and ensure interoperability and scalability of their AI solutions.

1.4. Cyber security threats in Banking

Cyber security threats in banks are the potential risks that could compromise the data, networks, and systems of financial institutions. Cyber security threats in banks could result in financial losses, reputational damage, regulatory penalties, and customer dissatisfaction. Some of the main threats/methods used against banks in cyberattacks include:

- Ransomware: This is a type of malware that encrypts the files or systems of the victim and demands a ransom for their decryption. Ransomware attacks can disrupt the operations and services of banks, as well as expose sensitive data. Ransomware attacks in the banking industry increased by 1318% in the first half of 2021.
- Phishing: This is a type of social engineering attack that uses fraudulent emails or websites to trick the recipients into revealing their personal or financial information, or clicking on malicious links or attachments. Phishing attacks can be used to steal credentials, money, or data from bank customers or employees.
- Trojans: These are malicious programs that disguise themselves as legitimate software or applications, but perform harmful actions once installed or executed. Trojans can be used to spy on, manipulate, or damage the data or systems of banks.
- Spoofing: This is a type of attack that involves impersonating a legitimate entity, such as a bank, a customer, or a vendor, to deceive the target into performing an action or providing information. Spoofing can be used to conduct fraudulent transactions, access restricted systems, or bypass security measures.
- Cyber security threats in banks are becoming more sophisticated and prevalent, as cybercriminals exploit the vulnerabilities and opportunities in the digital economy. Banks need to adopt a proactive and holistic approach to cyber security that covers all aspects of prevention, detection, response, and recovery. By doing so, banks can protect their assets, customers, and reputation from cyber attacks.

The advancement of computing technology has brought many benefits, but also some challenges. One of the major challenges is cybercrime, which is a new form of crime that uses information technology to commit fraud, theft, and other offenses. Cybercrime is increasing in number and variety, and it is difficult to monitor, control, detect, and prevent, as it transcends national borders and globalizes cybercrime. Information technology is both a tool and a target for cybercrime. Some cyber-attacks directly affect the systems of enterprises, such as phishing, which is hard to detect. To mitigate this problem, AI software tries to identify the behavioral patterns of all user accounts or devices.

AI can also enhance the security automation and integration of diverse products, which can offer key advantages. AI can improve the response time, optimize the scarce resources, and increase the productivity of the skilled security engineers. AI is based on human development and cutting-edge research, which can cope with all kinds of threats. AI can use advanced defensive capabilities to identify, mutate, and counter evolving threats within the network. AI labs can detect all threats. The banks' responses to cybercrime are analyzed, and the focus is shifted from single malicious agents and single points of attack to more complex scenarios. According to Crisanto and Prenio (2017), machine learning and AI provide unprecedented power to deal with unlimited budgets. To achieve high-quality cyber security in banks, it is important to examine the implementation of AI.

1.5. Uses of Arificial Intelligence in Banking system

Artificial intelligence (AI) is a technology that can perform various functions that are associated with human intelligence, such as reasoning, learning, interacting, creating, perceiving, and problem-solving. AI has many applications in the banking sector, such as:

- Customer service: AI can enable banks to provide 24/7 and personalized customer service through chatbots, voice assistants, and robo-advisors. AI can also help customers with onboarding, identity verification, account management, and product recommendations.
- Fraud detection and risk management: AI can help banks detect and prevent fraudulent transactions, cyberattacks, money laundering, and other forms of financial crime. AI can also help banks assess the creditworthiness of customers, monitor the market trends, and manage the regulatory compliance.
- Process automation and optimization: AI can help banks automate and optimize various processes, such as data entry, document analysis, report generation, loan underwriting, portfolio management, and payment processing. AI can also help banks reduce costs, errors, and delays.

AI is transforming the banking sector by enhancing the efficiency, quality, and security of the services. AI is also creating new opportunities for innovation and differentiation in the competitive market. AI is expected to have a significant impact on the future of banking.

- Enhancing customer interaction and experience: This category includes examples such as improving customer service, voice banking, robo-advice, biometric authentication, targeted customer offers, customer segmentation, and chatbots. These examples aim to provide more personalized, convenient, and engaging services to the customers.
- Improving efficiency of banking processes: This category includes examples such as predictive maintenance in IT, complaints management, automated data extraction, KYC, credit scoring, process automation/optimization, document classification, and more. These examples aim to streamline and optimize the various processes and operations of the banks.
- Developing security and risk control: This category includes examples such as AML (Anti-Money Laundering) detection and monitoring, enhanced risk control, support of data quality assurance, cyber risk prevention, compliance monitoring, payment transaction monitoring, fraud prevention, system capacity limit prediction, and more. These examples aim to protect the banks from cyber threats and financial risks.

In addition to these three categories, AI can also create new business opportunities and generate new sources of revenue for the banking sector. Some examples are investment analysis, personal finance management, asset allocation, lead generation, and more. These examples aim to explore new markets and offer new products and services to the customers.

1.6. Artificial intelligence in Banking

Artificial intelligence (AI) techniques are widely used in the financial services industry, especially in the customer-facing digital challenges. AI techniques enable machines to mimic human thinking, reasoning, and decision making. AI also helps the banks to improve innovation and lower costs by managing devices and data storage. However, as Byrnes stated in Technology Review, the technology still has some limitations in areas such as pattern recognition, image recognition, natural language processing, and hypothesis generation.

Credit scoring is one of the oldest applications of statistical modeling in the financial sector. It is not a new application, but it has been enhanced by AI techniques. Banks use statistical analysis, decision trees, regression, and transactional data to assess the credit risk of customers and provide suitable repayment methods. AI techniques improve the access and accuracy of credit scoring. They also reduce the risk and the number of false negatives and false positives. Banks can select the best debit plan for customers with the help of AI (Kose 2019). AI can also ensure the financial stability of banks by managing the credit risk. This is important because there are many supervisory requirements in this area, such as the European Banking Authority Regulatory Technical Standards in Assessment Methodology for an internal rating based Approach. These standards aim to achieve consistency and comparability in model outputs and risk-weighted exposures.

1.7. AI for customer interaction: the example of robo-advice and handling of customer complaints

Customer interaction is one of the key aspects of customer service, as it can influence customer satisfaction, loyalty, and retention. However, customer interaction can also be challenging, as customers have different needs, preferences, and expectations. Moreover, customer interaction can be costly and time-consuming for businesses, especially when dealing with large volumes of inquiries or complaints. Therefore, many businesses are looking for ways to leverage artificial intelligence (AI) to improve customer interaction and create more delightful experiences.

One example of AI for customer interaction is robo-advice, which is a form of automated financial advice that uses algorithms and data to provide personalized recommendations to customers. Robo-advice can help customers with various financial goals, such as saving, investing, retirement planning, or debt management. Robo-advice can offer several benefits for both customers and businesses, such as:

- Lower costs: Robo-advice can reduce the fees and commissions associated with traditional human advisors, making financial advice more accessible and affordable for customers. Robo-advice can also lower the operational costs for businesses, as they can serve more customers with fewer resources.
- Higher efficiency: Robo-advice can provide faster and more consistent service to customers, as it can process large amounts of data and generate recommendations in real time. Robo-advice can also eliminate human errors and biases that may affect the quality of advice.
- Better engagement: Robo-advice can enhance customer engagement by providing more personalized and relevant advice, based on the customer's profile, preferences, and behavior. Robo-advice can also use gamification, nudges, or rewards to motivate customers to follow their advice and achieve their financial goals.

Another example of AI for customer interaction is handling of customer complaints, which is a process of resolving the issues or problems that customers encounter with a product or service. Handling customer complaints can be a critical factor for customer satisfaction and retention, as well as for reputation and trust. However, handling customer complaints can also be a complex and stressful task for both customers and businesses, as it involves emotions, expectations, and communication. Therefore, many businesses are looking for ways to use AI to handle customer complaints more effectively and efficiently.

Some examples of AI for handling customer complaints are:

- Chatbots: These are AI-powered conversational agents that can interact with customers via text or voice. Chatbots can help customers with simple or common complaints, such as product returns, order cancellations, or account inquiries. Chatbots can also escalate complex or sensitive complaints to human agents when needed.
- Voice analysis: This is a technology that analyzes the voice of the customer or the agent to detect the tone and emotion. Voice analysis can help businesses understand the sentiment and satisfaction of customers, as well as the performance and stress level of agents. Voice analysis can also provide feedback or suggestions to improve the communication and resolution of complaints.
- Text analysis: This is a technology that analyzes the text of the customer feedback or reviews to extract the topics, opinions, and sentiments. Text analysis can help businesses identify the main sources and patterns of complaints, as well as the strengths and weaknesses of their products or services. Text analysis can also help businesses prioritize and respond to the most urgent or important complaints.

AI for customer interaction is a promising technology that can transform the way businesses communicate with and serve their customers. By using AI for robo-advice and handling of customer complaints, businesses can improve their customer service quality, efficiency, and engagement. However, AI for customer interaction also has some challenges and limitations, such as ethical, legal, social, and technical issues. Therefore, businesses need to carefully design, implement, and evaluate their AI solutions for customer interaction, and ensure that they complement rather than replace human agents.

2. Example of using ai to combat cyber security

Before development of chatbots, chatbots for Customer Suppport Mapa research was conducted successfully. To break down their utilization over the managing of any account part and different enterprise ventures of customers is targeted widely. Therefore, it is observed that chatbots are dispatched by Bank of America, American Express, and MasterCard, due to the helping customers explore applications all the more viable, customer questions speedier and providing help to consumers more cost viable. In addition, in the case of computerized reasoning, it is observed that this process is rotated around client support. Both in money related administration and past are presented with a large number of illustrations; these are not completely falsely insightful. According to Castelli et al. (2016), chatbots are conducted with the choice of trees; along with this acknowledge questions are unable to provide frequent replies toward the band's FAQs (Kanabolo and Gundeti, 2019). A few important managed learning processes are implemented; however, it is a long way from conscious robots of sci-fi. The property innovation process is introduced by banks that can maintain destination outsider edge (Facebook Messenger), application (for example, Barclays Launchpad, for instance) and destination, on the other hand, chatbots, are propelled by Facebook.

3. Advantages of artificial intelligence for the banking sector

AI techniques can help banks to analyze the expense patterns of customers and offer them customized investment plans that suit their budgeting plans. Banks can also inform customers about their spending and saving habits based on data. AI technology can track and understand the behavior and preferences of customers by using both traditional and alternative data sources. This can improve the employee experience as well (Cidon et al. 2019).

AI techniques can process and identify patterns from a large amount of data that may be missed by human observers. AI can play a vital role in fraud prevention by using machine learning solutions that can detect and prevent fraud in real time. Many financial service providers are developing and using AI techniques for this purpose.

Online banking or mobile banking is popular as it allows customers to make transactions anytime and anywhere. Banks can use AI techniques to access and analyze customer data from various sources, such as demographics, online and offline transactions, and website analytics. This can help banks to provide more personalized and relevant services to customers.

Risk assessment is a complex and critical process that requires accuracy and confidentiality when providing loans. AI techniques can handle the risk assessment process easily by analyzing the relevant data of customers. AI techniques can use information such as the latest transactions, credit history, social media activity, and other factors to evaluate the credit risk of customers (Agarwal 2019).

4. Disadvantages of ai for banking sector

- High cost: AI systems require high investment and maintenance costs, as they are complex and need regular updates and upgrades. AI systems may also need human supervision and intervention in case of failures or errors.
- Ethical and social issues: AI systems may raise ethical and social concerns, such as privacy, bias, accountability, transparency, and trust. AI systems may collect and use sensitive customer data, which may pose risks of data breaches or misuse. AI systems may also exhibit bias or discrimination based on the data or algorithms they use. AI systems may also lack human empathy, judgment, or explainability, which may affect customer satisfaction and loyalty.
- Job displacement: AI systems may replace human workers in some tasks or roles, such as customer service, fraud detection, or risk assessment. This may lead to job losses, skill gaps, or reduced human interaction in the banking sector. AI systems may also create new skills and roles that require training and adaptation.

5. Conclusion

Cyber threats are a serious challenge for the banking and financial sector, as they can cause financial losses, reputational damage, regulatory penalties, and customer dissatisfaction. To cope with these challenges, the banking and financial sector has adopted artificial intelligence (AI) as a promising technology that can enhance the cyber security and cybercrime prevention. AI can perform various functions that are associated with human intelligence, such as reasoning, learning, interacting, creating, perceiving, and problem-solving. AI can also handle large volumes of structured and unstructured data, extract useful patterns and insights, and control individual human behavior, inference methods, and knowledge representation.

This paper has explored the applications and implications of AI in the context of cyber security and cybercrime prevention. It has discussed the various methods and techniques of AI that are used to execute various tasks and solve problems related to cyber security. It has also analyzed the benefits and drawbacks of AI in the banking and financial sector, and suggested some ways to improve the performance and reliability of AI systems.

AI is transforming the cyber security and cybercrime prevention in the banking and financial sector by enhancing the efficiency, quality, and security of the services. AI is also creating new opportunities for innovation and differentiation in the competitive market. AI is expected to have a significant impact on the future of cyber security and cybercrime prevention. However, AI also has some challenges and limitations, such as ethical, legal, social, and technical issues. Therefore, businesses need to carefully design, implement, and evaluate their AI solutions for cyber security and cybercrime prevention, and ensure that they complement rather than replace human agents.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Agarwal, P., 2019, March. Redefining Banking and Financial Industry through the application of Computational Intelligence. In 2019 Advances in Science and Engineering Technology International Conferences (ASET) (pp. 1-5). IEEE.

[2] Dhashanamoorthi, Balaji. "Artificial Intelligence in combating cyber threats in Banking and Financial services." International Journal of Science and Research Archive 4.1 (2021): 210-216.

[3] Castelli, M., Manzoni, L. and Popovič, A., 2016. An artificial intelligence system to predict quality of service in banking organizations. Computational intelligence and neuroscience, 2016.

[4] Dhashanamoorthi, Balaji. "Resolving insurance claims with Artificial Intelligence powered decision making." International Journal of Science and Research Archive 10.2 (2023): 255-271.

[5] Cidon, A., Gavish, L. and Perone, M., Barracuda Networks Inc, 2019. System and method for ai-based anti-fraud user training and protection. U.S. Patent Application 15/693,353.

[6] Crisanto, J.C. and Prenio, J., 2017. Regulatory approaches to enhance banks' cybersecurity frameworks. Financial Stability Institutions (FSI) Insights on policy implementation, (2).

[7] Dimitrios, K., 2019. Can artificial intelligence replace whistle-blowers in the business sector?. International Journal of Technology Policy and Law, 3(2), pp.160-171.

[8] FSB (2017). Artificial intelligence and machine learning in financial services: Market developments and financial stability implications.

[9] Dhashanamoorthi, Balaji. "Opportunities and challenges of artificial intelligence in banking and financial services." International Journal of Science and Research Archive 10.2 (2023): 272-279.

[10] Humphrey, David B., Magnus Willesson, Göran Bergendahl and Ted Lindblom (2003). Cost Savings from Electronic Payments and ATMs in Europe. FRB of Philadelphia Working Paper No. 03-16.

[11] Bathaee, Yavar (2018). The Artificial Intelligence Black Box and the Failure of Intent and Causation. Harvard Journal of Law & Technology, 31 (2), 889-938.

[12] Inaba, Takashi and Mariagrazia Squicciarini (2017). ICT: A new taxonomy based on the international patent classification. OECD Science, Technology and Industry Working Papers, 2017/01. OECD Publishing, Paris.

[13] Dhashanamoorthi, Balaji. "Analyzing detection algorithms for cybersecurity in financial institutions." International Journal of Science and Research Archive 11.2 (2024): 558-568.

[14] F. Königstorfer and S. Thalmann, "Applications of Artificial Intelligencein commercial banks – A research agenda for behavioral finance" J BehavExp Finance, vol. 27, Sep. 2020

[15] A. Vaswani et al., "Attention Is All You Need," Jun. 2017[Online]. Available: http://arxiv.org/abs/1706.03762. [Accessed May. 2, 2024].

[16] A. R. Openai, K. N. Openai, T. S. Openai, and I. S. Openai, "ImprovingLanguage Understanding by Generative Pre-Training" 2018. [Online]. Available: https://s3-us-west-2.amazonaws.com/openai-assets/research-covers/language-unsupervised/language_understanding_paper.pdf.[Accessed May. 2, 2024].

[17] A. Radford, J. Wu, R. Child, D. Luan, D. Amodei, and I. Sutskever,"Language Models are Unsupervised Multitask Learners" 2018. [Online].Available: https://d4mucfpksywv.cloudfront.net/better-language-models/language_models_are_unsupervised_multitask_learners.pdf.[Accessed May. 2, 2024].

[18] T. B. Brown et al., "Language Models are Few-Shot Learners" 2020. [Online]. Available: https://arxiv.org/abs/2005.14165. [Accessed May. 2,2024].

[19] A. Q. Jiang et al., "Mixtral of Experts" Jan. 2024. [Online]. Available:https://arxiv.org/abs/2401.04088. [Accessed May. 2, 2024].