IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 13, Issue 2, April-May 2025
ISSN: 2320 – 8791 (Impact Factor: 2.317)
www.ijreat.org

AI-POWERED CYBER DEFENSE IN BANKING: IDENTIFYING, PREVENTING, AND RESPONDING TO CYBER THREATS

Mr. M. SaravanaKumar M.E 1, S. Parameshwari 2

1 Assistance Professor, Department of Computer Science and Engineering

Vandayar Engineering College

Thanjavur, Tamilnadu-613501, India

2 PG Student, Department of Computer Science and Engineering

Vandayar Engineering College

Thanjavur, Tamilnadu-613501, India

Paramesh101997@gmail.com

ABSTRACT

The growing digitization in the finance and banking sector has heightened the risk of cyber threats, making cybersecurity a critical concern. This paper investigates the application of machine learning models in the banking sector to safeguard sensitive financial data, prevent fraud, and ensure the integrity of digital Transaction. where machine learning enables banks to analyze vast amounts of transactional data and identify patterns associated with cyber threats. In Which Supervised learning is employed to detect known threats and flag suspicious activities, while unsupervised learning and anomaly detection help in identifying Unknown and emerging threats in real-time. There are challenges and complexity remain in the banking sector, using machine learning models. This paper emphasizes the necessity for ongoing research and the development of robust machine learning frameworks to ensure effective, adaptive, and secure cybersecurity solutions in finance and banking.

Key words: Machine Learning, Real-time cyber security, Artificial intelligence, Banking.

INTRODUCTION

In the digital age, banks and financial institutions face an unprecedented volume of cyberthreats. They have become prime targets for cybercriminals employing increasingly sophisticated attack methods. AI- powered cyber defense has emerged as a vital solution to bolster cybersecurity in the banking sector. Through artificial intelligence and machine learning, banks can identify, prevent, and respond to cyber threats more efficiently and effectively than ever before. This technology allows for real-time threat detection, predictive analytics, and automated responses, significantly reduce. This introduction explores how AI-powered cyber defense

solutions are transforming banking cybersecurity. AI-based cyber defense in banking is a critical step forward in protecting financial institutions and their clients from an ever-growing landscape of cyber risks. This Paper aims to Explore the application and implications of Artificial intelligence in the context of cyber security and cybercrime Prevention.

LITERATURE REVIEW

2.1. Use of AI in the Banking Sector

Author: Khalifa AL-Dosari, Published: 23 Aug 2022

AI is an umbrella term comprising a range of techniques and methods aiming to reproduce complex capabilities, such as autonomous decision-making and language. Machine learning (ML) is a subset of AI aimed at discovering patterns in data and making decisions.ML can be divided into supervised and unsupervised learning, based on whether the system is explicitly told the correct answers. Deep learning (DL) uses neural networks to perform highly complex information processing. AI allows for the use of advanced analytical tools and innovative business solutions in the banking sector. AI-powered systems make it possible for banks to develop multichannel customer access, gain insight into customer preferences, and tailor services to customer. The financial sector has become more competitive with the rise of FinTech companies. Banks are expected to implement innovative solutions and appropriate security measures for ensuring the privacy of their customers' information and meeting the needs of their customers. However, incumbent banks are at an inherent disadvantage compared to new FinTech firms when it comes to using new technologies. Banks may struggle to adapt, due to the established practices impairing the implementation of new technologies. This may create additional security risks, due to legacy financial and security software systems being incompatible with innovative solutions.

2.2. Cyber Security in Financial Sector Management (CS-FSM)

Author: Shailendra Mishra, Published: 10 May 2

Cybersecurity is necessary to safeguard a system, network, and technology against illegal access. In today's technologically advanced world, a company must have a dedicated cybersecurity team to monitor potential cyber threats and devise strategies for countering them. The essential elements of cybersecurity. Cybersecurity mainly includes secure payment, the online privacy of the user, an antivirus firewall, mobile security, security padlock, data protection, computer protection, and a specific global shield. For any company that processes electronic payments or transactions, payment security is critical to information security keeping abreast of the most recent developments in e-commerce and secure transaction methodology based on artificial intelligence, in particular the K-Nearest Neighbor (KNN) algorithm and the Enhanced Encryption Standard (EES) encryption and decryption algorithm, has been used to accomplish the research's goals.

Fig 2.2 Essential elements of cybersecurity in financial management.

2.3 AI in Cybersecurity

Artificial intelligence's spam filtering flags inappropriate content in every incoming communication. Malware can be detected due to its ability to learn and adapt. This harmful software is immediately recognized, and users are warned not to open any emails that include it. Utilizing data layering, deletion, and backup storage, companies can protect their software and platform activities through folder security. Encryption, tokenization, biometric verification, and essential control are other options. Protecting a financial institution's architecture by avoiding a wide range of dangerous threats from entering or spreading within a network is the goal of network security and can be accomplished by way of a collection of approaches. To preserve network safety, users need various types of network security (endpoint, online, wireless) and network security (firewalls, VPN encryption). Behavior analysis uses multiple techniques including machine learning, artificial intelligence, big data, and statistics.

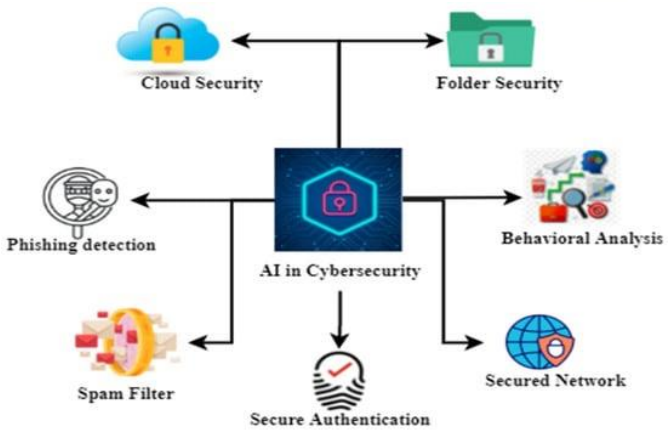

Fig 2.3 AI in cybersecurity.

2.4. AI in Identifying Cyber Threats

Author: Mohammad Binhammad, Shaikha Alqaydi, Azzam Othman, Laila Hatim

Abuljadayel Journal of Information Security Vol.15 No.2, April 30, 2024.

AI system excel in threat identification through their ability to analyze large datasets in real-time and identify deviations from established patterns.AI technologies like machine learning (ML) and natural language processing (NLP) have proven effective in identifying threats through anomaly detection, predictive analytics, and threat intelligence.

2.4.1 Anomaly Detection:

AI systems can analyze network traffic and transaction patterns in real-time flagging deviations that may indicate malicious activity. Unsupervised learning techniques, such as clustering and autoencoders, are commonly used for detecting anomalies in large datasets. Utilizing artificial intelligence algorithms to continuously monitor and detect anomalies in user behaviour transaction patterns and network activities, enabling swift identification of potential security threats. Anomaly detection is crucial in cyber security, identifying potential threats that break out of normal systems or networks.

2.4.2 Threat Intelligence:

Author: Mohammad Binhammad, Shaikha Alqaydi, Azzam Othman, Laila Hatim

Abuljadayel Journal of Information Security Vol.15 No.2 , April 30, 2024.

AI can parse vast amounts of unstructured data from online forums, dark web sites, and social media to identify potential threats before they materialize. NLP models are instrumental in extracting actionable intelligence from textual data.Establishing collaborative platforms for financial institutions to share real-time threat

intelligence enabling proactive response to emerging cyber threats across the industry. Those procedures involving collecting, analyzing, and comprehending information on potential or concrete cyber threats refer to cyber threat intelligence, a crucial element of cyber security. It assists organizations' triage processes in identifying actors' methods, techniques, and plans (TTPs) and recognizing the most `appropriate solutions to protect systems and data.

Organization Financial Institution	Threat Intelligence
	Utilizes AI for real-time monitoring of threats and vulnerabilities in the financial sector, providing timely insights to enhance security measures and protect against cyber-attacks.
Healthcare Provider	Uses AI to analyze threat intelligence data and identify potential security threats and vulnerabilities in medical systems and devices, ensuring patient data privacy and security.

Table 1: Threat Intelligence in different organizations

2.5 Vulnerability Management

AI tools like Tenable.io utilize machine learning to prioritize vulnerabilities in banking systems, ensuring issues are addressed promptly. Vulnerability management is a crucial aspect of cyber security, where it identifies, evaluates, and mitigates vulnerabilities, namely, a weakness, flaw, or error in a system or application. Similarly, AI has extensively automated weakness detection techniques, allowing companies to eliminate and count the vulnerabilities in order of their significance.

AI plays a crucial role in vulnerability management by ranking threats based on their severity and potential damage risks. AI algorithms can perform risk scoring and coordinate vulnerabilities based on risk level and compromise potential. This tool automates the process and reduces human labor in finding and protecting vulnerabilities. AI-powered frameworks can automatically identify system and application vulnerabilities and provide remediation recommendations. AI also enhances the precision of vulnerability management by minimizing unneeded positives. By analyzing multiple data sources simultaneously, AI algorithms can identify actual vulnerabilities more precisely, resulting in fewer false alarms.

AI has facilitated the transition to vulnerability management, making the detection and prioritization of cyber security weaknesses more precise. It is a powerful tool for organizations to sensitize vulnerability vigilance and protect against cyber threats.

Organization Financial Institution	Vulnerability Management
	Utilizes AI to automate vulnerability scanning and assessment processes, identifying and prioritizing vulnerabilities based on risk and potential impact.
Healthcare Provider	AI is used for analyzing security vulnerabilities occurring in medical devices and systems; high patches and updates protect the risk of cyber-attacks and data breaches would be in a position.

Table 2: Vulnerability Management in different organizations.

2.6. Fraud Detection

Cyber security and financial security nurture the effectiveness of fraud detection,

which is actually about detecting and preventing fraud, e.g., identity thefts, check fraud and account takeovers. Over the years, AI has been instrumental in boosting fraud detection in multiple organizations. It provides the ability to analyze large volumes of data in real-time, determine characteristics likely to be associated with fraudulent behaviours and take the necessary measures to avoid crimes.

Deriving from the AI's powerful capabilities for fraud detection is the quality to
process and extract relevant information from multiple sources and, consequently, to under, and intricate and unexpected patterns of fraudulent activity. Human computers can use AI systems' data analysis skills to easily detect anything suspicious, such as transactions, behaviour, and historical patterns, to afford them more time for further investigation.

CONCLUSION

According to the research paper, cyberattacks are likely to intensify and become more sophisticated in the coming years. Therefore, it is essential to be prepared and employ new technology tools such as artificial intelligence and cybersecurity to protect sensitive data at all levels, from personal to business to government and entire nations. Every country in the world needs to establish initiatives to raise public awareness of new technologies and provide funding for their development. The current study aimed to demonstrate the importance of cybersecurity and artificial intelligence in preventing internet threats. Artificial intelligence can help create a safer work environment, as it can be used in the front office, middle-office, and back-office departments of any industry where there are lots of computer-to-computer interactions. However, people may still be the weakest link in a cybersecurity system.

REFERENCE

[1] N. R. Mosteanu, "Artificial intelligence and cyber security–face to face with the cyberattack–a maltese case of risk management approach," Ecoforum Journal, vol. 9, no. 2, 2020.

[2] "Malta accuses Russia of cyber-attacks in the run-up to the election,"The Guardian, 27-May-2017.

[3] N. R. Mosteanu, "Artificial Intelligence and Cyber Security–A Shield against Cyberattack as a Risk Business Management Tool–Case of European Countries," Quality-Access to Success, vol. 21, no. 175,2020.

[4]. X. Qiu, Z. Du and X. Sun, " Artificial Intelligence-Based Security Authentication:Applications in Wireless Multimedia Networks," in IEEE Access, vol. 7, pp.172004- 172011, 2019, doi:10.1109/ACCESS.2019.2956480.

[5] D. Faggella, "Artificial Intelligence in finance - A comprehensive overview," Emerj Artificial Intelligence Research, Dec. 24, 2019.

[6] Abrahams, T.O., Farayola, O.A., Kaggwa, S., Uwaoma, P.U., Hassan, A.O., & Dawodu, S.O. (2024). Cybersecurity awareness and education programs: a review of employee engagement and accountability. *Computer Science & IT Research Journal*, *5*(1), 100-119.

[7] Adil, M., Song, H., Mastorakis, S., Abulkasim, H., Farouk, A., & Jin, Z. (2023). UAV-Assisted IoT applications, cybersecurity threats, ai-enabled solutions, open challenges with future research directions. *IEEE Transactions on Intelligent Vehicles*.

[8] Ahmad, I.A.I., Anyanwu, A.C., Onwusinkwue, S., Dawodu, S.O., Akagha, O.V., & Ejairu, E. (2024). Cybersecurity challenges in smart cities: a case review of african metropolises. *Computer Science & IT Research Journal*, *5*(2), 254-269.

[9] Alevizos, L., & Dekker, M. (2024). Towards an AI-Enhanced Cyber Threat Intelligence Processing Pipeline. *arXiv preprint arXiv:2403.03265*.

[10] Allam, Z., & Allam, Z. (2021). Big data, artificial intelligence and the rise of autonomous smart cities. *The rise of autonomous smart cities: technology, economic performance and climate resilience*, 7-30.