International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 12 Issue 1, January, 2023, Impact Factor: 7.751

The Role of Artificial Intelligence in Enhancing Cybersecurity Measures in Online Banking Using AI

Archana Todupunuri

Fidelity Information Services, USA

ABSTRACT

The research attempt to investigate the role of AI in hardening cybersecurity within the United States online banking sector. The study gives an assessment of the effectiveness regarding the usage of AI for detecting and mitigating risks arising out of cybersecurity by comparing different AI-driven methods against their traditional counterparts, to outline the respective benefits and limitations. Additionally, it touches on the opportunity that AI-based cybersecurity presents in protecting other online banking industries of the US. These findings underlined the adaptability of AI in fighting these ever-evolving threats, even as resource demands are uniquely challenging. This study underlines the transformative potential of AI within proactive digital defence.

Keywords: Online banking, U.S. industries, Artificial intelligence, Digital threats, Cybersecurity

INTRODUCTION

Online banking has grown dramatically, making it easy and available to any user from anywhere in the world. However, this exponential rise in digital banking has also increased the risks involved, particularly in cybersecurity. Online banking systems remain a target for cyber-criminals that can attempt phishing, identity theft, and unauthorised access [1]. So, there is an immediate need to consider security imperatives. Artificial intelligence has recently emerged as a very strong tool for enhancing cybersecurity, offering higher-order threat detection, response, and mitigation. Machine learning and anomaly detection, among other AI-driven technologies, have immense potential for identifying suspicious activities and reducing fraud in real time. Adapting these systems to the dynamic landscape of cyber threats still seems to have its fair share of challenges despite the promise that AI rides on regarding cybersecurity. The research enumerates deeper ramifications of AI-enhanced security measures for the other online banking sectors in the U.S.

AIMS AND OBJECTIVE

Aim

This study aims to assess the usefulness of artificial intelligence in improving cybersecurity measures in online banking, as well as the larger implications for crucial industries in the United States.

Objectives

- To examine the current cybersecurity concerns confronting the United States online banking sector
- To determine the efficacy of artificial intelligence in identifying and mitigating online banking risks
- To compare AI-driven cybersecurity measures to traditional ways in online banking
- To investigate the possible applications of AI-enhanced cybersecurity solutions in other vital US industries

RESEARCH QUESTIONS

- What are the current cybersecurity concerns of the online banking sector in the United States?
- How does AI handle the issues of detection and mitigation of cybersecurity risks in online banking?
- What does AI-driven cybersecurity contrast with traditional methods in online banking?

- What can be some additional uses of AI-enhanced cybersecurity solutions in other online banking sectors and industries in the United States?

LITERATURE REVIEW

Cybersecurity Challenges in the U.S. Online Banking Sector

The rapid growth of digital transactions and the changing dimensions of cyber threats are critically testing cybersecurity in the U.S. online banking sector. Financial institutions turn out to be potential targets of cybercriminals who adopt various tactics like phishing malware attacks and social engineering [2]. These methods can easily be utilised to take advantage of vulnerabilities in the system that too often result in unauthorised access, financial theft, and compromising customer data. This has been exacerbated by the increase in mobile banking and other ways of digital payment; mobile devices are easy to attack. Secondly, regulatory compliance for the realisation of cybersecurity standards imposed by federal authorities also adds to the level of complexity for banks in the protection of sensitive information [3]. Conveniences to its users have to be weighed against stringent security measures in the sector such as increased security controls can impede user experience. The different higher-order ways of committing cybercrimes are committed and traditional ways of security become less effective. Advanced cybersecurity strategies are greater in demand as a way to further strengthen defences against the evolving threats of online banking to be sure of featuring artificial intelligence.

Efficacy of Artificial Intelligence in Identifying and Mitigating Online Banking Risks

There is promise in formulating and reducing cybersecurity risks within online banking with Artificial Intelligence. AI can analyse a vast volume of transaction data in real time to determine unethical behaviour that can show fraud or other security breaches [4]. Advanced algorithms enable systems to learn from history, whereby the precision of the prediction and prevention improves over time, enabled by machine learning models. Other benefits involve the provision of better threat detection with patterns associated with malware, phishing attempts, or unauthorised accesses that can have passed traditional methods of detection. AI can adapt to new and constant threats by offering a dynamic cyber defence against tactics perpetuated by cybercriminals. Automation of AI systems in threat detection and response provides a reduced level of human error by way of quicker, deeper mitigation of the associated risks [5]. Other challenges with AI in cybersecurity include false positives or the way to handle data privacy. AI has nonetheless become invaluable in securing highly targeted online banking.

Comparison of AI-Driven and Traditional Cybersecurity Measures in Online Banking

AI-powered cybersecurity in online banking gives a whole bunch of advantages compared to traditional techniques, mainly in the insight it offers into threats. Traditional cybersecurity relies on rule-based systems or signature detection good enough in the case of detecting known threats but often poor in the case of newly created sophisticated types of attacks [6]. Methods of security face challenges while being very traditional to find anomalies in real-time and can leave opportunities for cybercriminals to use against them. On the other hand, AI-driven systems involve the activation of continuous learning with machine learning and anomaly detection, automatically adapting to new patterns without human intervention. Complex behavioural patterns can be analysed, enabling the early detection of irregular activities that can go unnoticed by traditional methods with AI.

It also minimises the need for constant human oversight in threat response and detection reducing response times with a view of limiting the impact that a potential breach can cause. However, AI systems can also suffer from related problems of false positives. Another limitation of AI-driven approaches is that they usually require heavier computational resources and training data compared to conventional methods [7]. Adaptability or precision, AI-driven cybersecurity measures are well-programmed to act as an imperative addition in conventional defence against the ever-growing complex cyber-attack in online banking.

Cross-Industry Applications of AI-Enhanced Cybersecurity in U.S. Online Banking Sectors

The implications of AI-enhanced cybersecurity go beyond online banking in many important areas for the U.S. Artificial intelligence-enhanced cybersecurity plays a vital role in U.S. online banking today, putting huge emphasis on detecting fraudulent patterns and preventing all types of cyberattacks. Advanced algorithms run constant analytics on data in real time to identify suspicious transactions and unauthorized access. Automation of threat detection and response by AI helps banks guard sensitive information and create secure digital interactions for customers while driving operational efficiency in cybersecurity management.This can provide machine-learning algorithms capable of spotting and flagging suspicious activities in real-time to prevent such cyberattacks as ransomware attacks or unauthorised access to banking records. AI is used to protect Online Bankinginfrastructures from cyber-attacks that can down a country's power grid or energy network in the energy sector [8].AI-powered cybersecurity in the U.S. online banking industry enhances the notion of fraud detection and prevention through real-time analyses of transactional patterns. Anomaly identification, with the help of

machine learning algorithms, along with possible threats, enables quicker responses against cyberattacks. These AI-driven solutions have significantly improved system resilience, protected sensitive financial information, reduced manual oversight, and created a far more secure and efficient banking environment for customers.AI-driven cybersecurity becomes integral protection for government and defence systems from advanced persistent threats [9]. The following industries listed enjoy the adaptability, scalability and real-time capabilities of threat detection provided through AI. AI offers an all-around proactive approach to ever-evolving sophisticated cyber threats that can be leveraged across various.

METHODOLOGY

The methodology applied in the present research is embedded in the ***interpretivism philosophy*** and can seek to understand social phenomena and AI-enhanced cybersecurity, through varied stakeholder perspectives about online banking. Interpretivism allows for the exploration of complex issues in detail recognition and consideration of the subjective experiences of individuals concerned regarding cybersecurity measures [10]. A ***deductive approach*** is adopted, where existing theories concerning the effectiveness of AI in solving the Cybersecurity challenges being faced by the online banking sector are tested. The approach can confirm findings or oppose the established views with evidence based on secondary sources of data.

The information utilised for research was based on ***secondary data*** such as academic journals, reports from industries and analyses by experts. This can provide deep insight into the way the aspects of cybersecurity and AI are interfacing with the latest developments in online banking. Secondary data is better since it is more accessible, dependable and well-known in the area [11]. This also allows for the analysis of a wide range of views that cannot be possible with primary data.

Thematic analysis represents the major approach that was used in the machine learning analytical method in this study. This includes the identification, analysis, and reporting of patterns within the data. The ***thematic analysis*** can be applicable because it gives a flexible way of interpreting qualitative data. It can ascertain the way repeated themes about AI in cybersecurity are developed. ***Qualitative thematic analyses*** allow deep insights into the nuanced roles that AI can play in cybersecurity measures and provide insight into the way this can affect the online banking sector. This approach connotes the research aims to explore and understand complex issues in-depth rather than merely quantify them.

DATA ANALYSIS

Theme 1: The current cybersecurity risks and difficulties confronting the US online banking business are examined.
Contemporary cybersecurity risks and challenges for US online banking remain complex and dynamic. Online banking, being the vanguard of digital money, is particularly vulnerable to illicit activities such as phishing, malware, and ransomware assaults. These attacks are especially targeting weaknesses in financial systems, mobile applications, and third-party service providers. The foreseen cyber threats that are still prevalent and a major concern for Online banking include unauthorised access to sensitive customer information, mainly financial [12]. Another threat in the sector arises from the rising cases of identity theft where fraudsters assume the identity of another person to get unauthorised access to their bank accounts. This sets off a challenge that banks grapple with in trying to find an appropriate balance between seeking the use of convenience by users and compelling security measures. The complexity of securing mobile devices and payment platforms is further reaching its limits with the general increase of digital banking. Regulatory compliance is a consideration whereby different standards ensure that customer information is protected and security-sound [13]. The fast growth of online financial services is increasing the attack surface so that the attackers can carry out an effective attack such as superior protection mechanisms are needed. On the other hand, it speaks to the need for constant innovation in cybersecurity strategies to protect FIs and their customers.

Theme 2: The efficiency of artificial intelligence for recognising and managing hazards in online banking is assessed.
Efficiency AI can be easily distinguished from the recognition and management of online banking risks. More specifically, AI systems may process millions of transaction data in real time using machine learning algorithms. AI finds uncommon patterns- probably fraudulent activities included- providing an efficient mechanism of defense against cyber threats. The accuracy of AI in predicting and preventing risks in the future continues to get better with the use of burgeoning historical data [14]. For example, AI can identify anomalies in transaction behaviour, such as transactions at strange hours of the day or large-scale fund transfers, as a source of potential fraud. Artificial intelligence-driven solutions improve phishing detection by analysing communication patterns and flagging suspicious activities. Detection allows automatic response by giving way to reduce human intervention and minimising response times with AI tools [15]. This greatly reduces human errors that usually are the weakest link in conventional cybersecurity practices. However, AI effectiveness depends on the data quality and continuous training of the system. AI has become anOnline Banking strategic component in improving

cybersecurity in online banking. It allows for proactive steps that are consistent with the dynamic and growing nature of digital threats despite certain obstacles.

Theme 3: AI-powered cybersecurity techniques are contrasted with conventional cybersecurity approaches utilized in online banking.

AI cybersecurity technique helps online banking much more than the traditional cybersecurity approach in several ways, including that the traditional techniques depend on certain predefined rules and signature-based detection. This can identify only known threats, having a very minimal capability in detecting new or advanced types of cyberattacks. However, AI-based systems apply machine learning algorithms to analyze big datasets for complex patterns and behaviours that denote emerging threats [16]. The continuous learning against new risks with AI means that threat detection improves with time. AI can detect anomalies in real-time faster compared to traditional systems, where the analysis manually may take a little time.

Most of the methods of cybersecurity have conventionally relied on human intervention and are susceptible to latency in response with high chances of errors. Automation through artificial intelligence diminishes the scope of human error instantaneous threat detection and response [17]. The AI-driven systems can nest across a wide attack surface, including phishing, malware and insider threats. Traditional cybersecurity methods often are unable to keep pace with an ever-changing cyber threat landscape.

Theme 4: The potential use of AI-enhanced cybersecurity solutions in other vital US businesses is investigated.

The necessary steps to take further consideration for expanded use beyond online banking of AI-enhanced cybersecurity solutions in other key industries within the U.S. where the benefit appears considerable. Artificial intelligence can shield sensitive data from various forms of cyberattacks and data breaches [18]. The energy sector also benefits from this angle such as AI secures Online Banking infrastructures of power grids and energy networks far from the hands of cyber threats. These AI mechanisms analyse volumes of operational data to detect any potential vulnerabilities that could cause system failure or attacks. AI-powered cybersecurity can help protect customer payment information from fraudsters through its tracking of transaction patterns and flagging suspicious activities accordingly [19]. AI can indeed be applied in the government and defence sectors to protect sensitive national security data from advanced persistent threats by applying, AI adapted and learned something new from each data point that came in, making this technology peculiarly apt for these sectors. Challenges persist in resource requirements and integration complexity with high stakes of cyber-attacks in such industries. Embracing AI-enhanced cybersecurity allows one to realise that an effective defence mechanism is scalable and proactive across many sectors. An urgent need for AI-powered solutions has been highlighted by the recent intensification of cyber threats to safeguard the Online Bankingindustries of the United States.

FUTURE DIRECTIONS

The future of AI and cybersecurity both embark on real-time threat detection to make online banking more secure in approaching customer transactions. It can be easier for banks to predict fraud and prevent breaches with advanced machine learning algorithms. Deep learning, further integrated can make the process of anomaly detection even smoother and reduce the risks of unauthorized access. Application of biometrics in banking, like facial and voice recognition can introduce a whole new level of security levels[20]. Blockchain deployment has been decentralized in securing transactions, hence making it all the more transparent. The collaboration of more institutions can drive a shared intelligence that fortifies general resilience in cybersecurity within online banking.

CONCLUSION

It can be concluded that AI has been irreplaceable in strengthening cybersecurity measures within online banking and other Online Bankingof the United States. The proficiency for real-time detection and adaptability in learning gives it a greater edge over traditional approaches. Many challenges remain concerning resource consumption and system complexity, proactive automated solutions fall on the positive side of AI. Innovation in AI-driven cybersecurity must accelerate to meet these evolving concerns as cyber threats change. This achievement is important for safeguarding sensitive data in banking and other businesses.

REFERENCES

[1]. Al-Badran, O.R.A., 2021. The impact of electronic crimes on the risks of banking financial services in light of the increasing use of banking information technology and communications. *Academy of Entrepreneurship Journal*, *27*(6), pp.1-10.

[2]. Marotta, A. and Madnick, S., 2021. Convergence and divergence of regulatory compliance and cybersecurity. *Issues in Information Systems*, *22*(1).
[3]. Nicholls, J., Kuppa, A. and Le-Khac, N.A., 2021. Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. *Ieee Access*, *9*, pp.163965-163986.
[4]. Munoko, I., Brown-Liburd, H.L. and Vasarhelyi, M., 2020. The ethical implications of using artificial intelligence in auditing. *Journal of business ethics*, *167*(2), pp.209-234.
[5]. Gudala, L., Shaik, M., Venkataramanan, S. and Sadhu, A.K.R., 2019. Leveraging Artificial Intelligence for Enhanced Threat Detection, Response, and Anomaly Identification in Resource-Constrained IoT Networks. *Distributed Learning and Broad Applications in Scientific Research*, *5*, pp.23-54.
[6]. Soe, Y.N., Feng, Y., Santosa, P.I., Hartanto, R. and Sakurai, K., 2019. Rule generation for signature based detection systems of cyber attacks in iot environments. *Bulletin of Networking, Computing, Systems, and Software*, *8*(2), pp.93-97.
[7]. Marda, V., 2018. Artificial intelligence policy in India: a framework for engaging the limits of data-driven decision-making. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *376*(2133), p.20180087.
[8]. SathishkumarChintala, Sandeep Reddy Narani, Madan Mohan Tito Ayyalasomayajula. (2018). Exploring Serverless Security: Identifying Security Risks and Implementing Best Practices. International Journal of Communication Networks and Information Security (IJCNIS), 10(3). Retrieved from https://www.ijcnis.org/index.php/ijcnis/article/view/7543
[9]. Narani, Sandeep Reddy, Madan Mohan Tito Ayyalasomayajula, and SathishkumarChintala. "Strategies For Migrating Large, Mission-Critical Database Workloads To The Cloud." Webology (ISSN: 1735-188X) 15.1 (2018).
[10]. Chirra, D.R., 2021. The Impact of AI on Cyber Defense Systems: A Study of Enhanced Detection and Response in Critical Infrastructure. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(2), pp.221-236.
[11]. Jimmy, F., 2021. Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses. *Valley International Journal Digital Library*, pp.564-574.
[12]. Shah, Hitali. "Ripple Routing Protocol (RPL) for routing in Internet of Things." International Journal of Research Radicals in Multidisciplinary Fields, ISSN: 2960-043X 1, no. 2 (2022): 105-111.
[13]. Hitali Shah.(2017). Built-in Testing for Component-Based Software Development. International Journal of New Media Studies: International Peer Reviewed Scholarly Indexed Journal, 4(2), 104–107. Retrieved from https://ijnms.com/index.php/ijnms/article/view/259
[14]. Alharahsheh, H.H. and Pius, A., 2020. A review of key paradigms: Positivism VS interpretivism. *Global Academic Journal of Humanities and Social Sciences*, *2*(3), pp.39-43.
[15]. Buder, S., Asplund, M., Duong, L., Kos, J., Lind, K., Ness, M.K., Sharma, S., Bland-Hawthorn, J., Casey, A.R., De Silva, G.M. and D'Orazi, V., 2018. The GALAH Survey: second data release. *Monthly Notices of the Royal Astronomical Society*, *478*(4), pp.4513-4552.
[16]. Gunduz, M.Z. and Das, R., 2020. Cyber-security on smart grid: Threats and potential solutions. *Computer networks*, *169*, p.107094.
[17]. Ayyalasomayajula, Madan Mohan Tito, SathishkumarChintala, and Sandeep Reddy Narani. "Intelligent Systems and Applications in Engineering.", 2022.
[18]. Abbott, K.W. and Snidal, D., 2021. The governance triangle: Regulatory standards institutions and the shadow of the state. In *The spectrum of international institutions* (pp. 52-91). Routledge.
[19]. Baryannis, G., Validi, S., Dani, S. and Antoniou, G., 2019. Supply chain risk management and artificial intelligence: state of the art and future research directions. *International journal of production research*, *57*(7), pp.2179-2202.
[20]. Wang, P., Berzin, T.M., Brown, J.R.G., Bharadwaj, S., Becq, A., Xiao, X., Liu, P., Li, L., Song, Y., Zhang, D. and Li, Y., 2019. Real-time automatic detection system increases colonoscopic polyp and adenoma detection rates: a prospective randomised controlled study. *Gut*, *68*(10), pp.1813-1819.
[21]. Sarker, I.H., 2021. Machine learning: Algorithms, real-world applications and research directions. *SN computer science*, *2*(3), p.160.
[22]. Shah, Hitali. "Ripple Routing Protocol (RPL) for routing in Internet of Things." International Journal of Research Radicals in Multidisciplinary Fields, ISSN: 2960-043X 1, no. 2 (2022): 105-111.
[23]. Er Amit Bhardwaj, Amardeep Singh Virdi, RK Sharma, Installation of Automatically Controlled Compensation Banks, International Journal of Enhanced Research in Science Technology & Engineering, 2013.
[24]. Raisch, S. and Krakowski, S., 2021. Artificial intelligence and management: The automation–augmentation paradox. *Academy of management review*, *46*(1), pp.192-210.

[25]. Meurisch, C. and Mühlhäuser, M., 2021. Data protection in AI services: A survey. *ACM Computing Surveys (CSUR)*, *54*(2), pp.1-38.

[26]. Khurana, R. and Kaul, D., 2019. Dynamic cybersecurity strategies for ai-enhanced ecommerce: A federated learning approach to data privacy. *Applied Research in Artificial Intelligence and Cloud Computing*, *2*(1), pp.32-43.

[27]. Wang, J.S., 2021. Exploring biometric identification in FinTech applications based on the modified TAM. *Financial Innovation*, *7*(1), p.42.