

Charting the Cybersecurity Landscape: A Systematic Literature Review of AI-Powered Chat Bots in Banking and Finance

Shruti Pawar¹ and Pranav Kulkarni²

¹⁻²Dr. Vishwanath Karad MIT World Peace University/Department of Computer Science, Pune, India
Email: shrutipawar216@gmail.com, pranavkulkarni06@gmail.com

Abstract—In the face of rapid technological advancements, the Banking and Finance sector finds itself at the forefront of escalating cybersecurity challenges. The imperative to safeguard sensitive information has driven organizations to bolster their cybersecurity posture, emphasizing the need for a robust culture of information security. In response to these challenges, there is a growing recognition of the role that chatbots, powered by Artificial Intelligence (AI) and Large Language Models (LLMs), can play in fortifying financial systems. With a primary focus on providing valuable insights to practitioners, researchers, and policymakers, the research aims to facilitate dynamic decision-making at the crucial intersection of cybersecurity and financial systems. The overarching goal is to identify and analyze existing and emerging themes, methodologies, and technologies in the research landscape, pinpointing trends, evolution, and key contributors in the scholarly discourse. The research also places a significant emphasis on ensuring compliance with existing implementations vis-à-vis regulatory requirements and government norms concerning legal implications in the use of AI-powered chatbots in the financial sector. This involves a thorough examination of the legal and regulatory landscape surrounding the deployment of chatbots, with a keen eye on ensuring ethical and lawful practices. To this study, reputable databases such as IEEE Xplore, Web of Science, and Scopus will be extensively utilized. Interpreting the results derived from these analyses will illuminate significant contributors, collaborative networks, and emerging trends pertaining to the research topic.

Index Terms— Cybersecurity, Chatbots, Systematic Literature Review (SLR), Financial Technology (FinTech), Natural Language Processing (NLP) and Vulnerability Assessment.

I. INTRODUCTION

In today's world there is a growing number of risks that pose a threat to people's finances stored in banks. This is why it is crucial for banks to leverage technology to safeguard their customers data and funds. Chatbots, assistants that engage with users online play a significant role in enhancing the security of banks against cyber threats. They are adept, at detecting risks educating customers on safe online practices providing prompt assistance when issues arise and monitoring critical banking systems. It is imperative for banks to embrace these tools not for customer interactions but primarily for bolstering security measures and outmanoeuvring cybercriminals. The increasing significance of chatbots can significantly boost client's confidence as well as data safety within the banking sector, providing a secure business experience, pertaining to the ongoing

transformations in the era of digitalization. With the rapid expansion of digital banking services and reliance on technology in the financial and banking sector, the need for robust cybersecurity measures has never been more critical, making chatbots a fantastic tool to enforce stringent cybersecurity policies in banking organizations. Recent hacking incidents like the Flex cube database attack by state sponsored hackers have banking institutions worldwide on high alert, highlighting the vulnerabilities in the banking system and the potential for massive financial losses. Chatbots function, as assistants that safeguard valuable data. They play a role in ensuring the security of information in financial institutions, like banks detecting any potential issues that arise. Regular maintenance and testing of chatbots are essential to verify their functionality and identify any vulnerabilities.

A. Rationale and Importance

In the evolving landscape of Banking and Finance Cybersecurity, the integration of chatbots poses opportunities as well as challenges. Issues stem from the need for a comprehensive understanding of the scholarly discourse surrounding the role of chatbots in bolstering cybersecurity measures. The target is to inform decision-makers, researchers, and industry practitioners about the trajectory of research in this field, through a systematic literature review, aiming to contribute vital insights essential for navigating the intersection of finance, and cybersecurity using chatbots, fostering more informed strategies for securing financial systems. The rationale for this research lies in addressing the gaps in existing literature, providing a consolidated view of contributors, and emerging trends.

B. Gap Analysis

The following gaps were identified while reviewing the existing literature-

Gaps were identified in the literature regarding the use of anthropomorphic chatbots as e-banking customer service. It is aimed to fill this gap by investigating the factors that influence the intention to use anthropomorphic chatbots in this context.

In the literature regarding the impact of AI-powered chatbots on digital financial inclusion, the gaps were identified which needs to be addressed by developing a conceptual framework for understanding this impact.

Gaps are present in the literature regarding the relationship between digital privacy concerns, trust, and user self-disclosure to chatbots in the context of the banking market.

The research in the area is concentrated around the USA, Central Europe, Southeast Asia, and southern and eastern African countries. Not much research has been done on the topic in the geographic regions of the UK, India, Australia, Japan, and Latin American countries.

C. Problems Identified

Problem 1: Investigation of factors affecting customer acceptance using a banking chatbot w.r.t factors such as perceptions and future adaptability (focusing on real-life errors and human likeness)

Problem 2: Examine the ability of Chatbots to adapt to dynamic and evolving cyber threat landscapes in the banking and finance industry.

Problem 3: Identify and analyze existing and emerging trends, encapsulating newer technologies in the research landscape of Chatbots for Cybersecurity in Banking and Finance.

Problem 4: GenAI is a technology designed to safeguard us from cyber threats. However, it does come with its drawbacks. One concern is its misuse by individuals to execute harmful cyber assaults. Chatbots such, as ChatGPT could be exploited by them to deceive and manipulate individuals online. Thus, although GenAI serves a role it also presents an avenue for actors to engage in malicious activities.

II. RESEARCH METHODOLOGY

A comprehensive search was conducted using academic databases such as Scopus Web of Science, and IEEE Xplore, as well as relevant publications from the financial industry like Bloomberg, McKinsey, and other company reports. The search utilized keywords and critical terms, including: AI-powered chatbots, chatbots, conversational AI, virtual assistants, banking, finance, fintech, cybersecurity, cyber vulnerabilities, cyber threats, risk management, data privacy, authentication, PCI-DSS, and encryption. Boolean operators (AND, OR, NOT) were employed in search strings to ensure a comprehensive and focused collection of relevant literature. Additionally, the reference lists of identified articles were manually scanned to find relevant studies not captured in the initial search.

A. Inclusion/ Exclusion Criteria

Inclusion: Peer-reviewed research articles, industry reports, and white papers published within the past five years (2019-2024) that primarily focus on the use and cybersecurity implications of AI-powered chatbots in banking and finance institutions.

Exclusion: Conference proceedings, book chapters, news articles, opinion pieces, and studies focusing on chatbot applications outside of banking and finance.

B. Selection Process

Articles identified through the search strategy were screened by title and abstract for relevance to the research questions. Full-text articles of initial hits were further assessed for eligibility based on the inclusion/exclusion criteria by two independent reviewers.

C. Data Analysis

The extracted data was coded and categorized based on themes and research questions. A qualitative analysis was conducted using thematic analysis and coding techniques, including tools like ConnectedPapers and LitMaps, to identify patterns and trends in the literature. The obtained facts were formulated, summarized, and documented in the standard IEEE format of a research paper.

III. LITERATURE REVIEW

Some of the key themes that are covered in the analysed papers include customer loyalty, e-commerce quality, mobile app usage, chatbots, human-chatbot relationships, and service quality. For example, in [14] the authors examine how service quality in mobile food delivery services impacts customer loyalty. Similarly, in [10], the authors explore the impact of e-commerce quality on customer satisfaction, loyalty, and perceived risk. In [7] the authors seek to understand the factors that influence customers' intention to continue using smartphone banking services. On the other hand, [5] examines the acceptance and use of retail mobile banking apps by South African millennials. Another area of focus is chatbots and human-chatbot relationships. In [16] the author investigates the impact of using banking chatbots on the customer experience and brand love; while in [4], the authors examine the relationship between humans and chatbots. The research includes papers on technology acceptance and usage, the authors analyze the factors that influence customer satisfaction during online shopping holidays. In [3] the authors propose a unified theory of technology acceptance and usage. The most recent regulatory guidelines for digital services and electronic transactions are specifically (Example: POJK Number 12/POJK.03/2018), emphasizing the subtle differences in laws between digital banking services and payment transaction processing are also considered. Large Language Models (LLMs) and their potential for cyber deception are covered in detail in the paper, where initial studies explore the intricacies of LLMs, emphasizing how they work best when combined with honeypots. his study in [1] [2] examines the intersection of digital financial inclusion and mobile phone technologies, focusing on their impact on stakeholders such as financial users, providers, governments, and the economy.

The role of human errors and socio-technical hurdles in cybersecurity are examined, advocating for increased awareness and effective measures within financial institutions. Furthermore, a systematic review of existing literature on chatbots is conducted, with a focus on security, privacy, data protection, and social dimensions. The review aims to offer a comprehensive understanding of the challenges and potential solutions in this field.

The study identifies ways to minimize security issues and contributes to the ongoing discourse on ensuring the robustness and privacy of chatbot technologies. Overall, these findings provide valuable insights into the dynamic landscapes of digital financial inclusion, mobile technologies, and chatbot literature, offering a nuanced understanding of challenges, opportunities, and potential paths forward in these evolving domains.

This literature also explores the evolution of Generative AI (GenAI) and its role in the cybersecurity landscape. It provides an overview of GenAI's development, emphasizing its significance and impact. The review critically examines GenAI's applications in cybersecurity, highlighting its transformative potential and inherent limitations. Specifically, vulnerabilities in the ChatGPT model are discussed, shedding light on possible security concerns. Additionally, the dual-use nature of GenAI is explored, considering both its defensive and offensive applications in cyber operations.

The review also explores the crafting and demonstration of common, easily deployable cyberattacks, emphasizing the practical implications of generative AI technologies. Overall, it highlights the importance of understanding multifaceted issues surrounding ChatGPT and other generative AI models, emphasizing ethical implications.

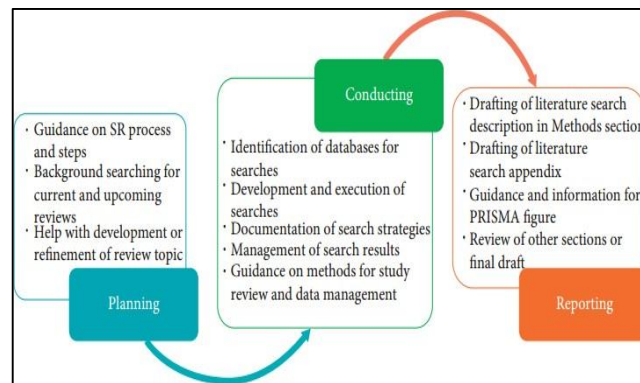


Figure 1. Systematic Review Process

IV. RESEARCH ANALYSIS, RESULTS AND KEY FINDINGS

Problem 1- Investigation of factors affecting customer acceptance using a banking chatbot with respect to factors such as perceptions & future adaptability (focusing on real-life and human errors) Using approaches like LGCM, partial least squares structural equation modelling (PLS-SEM), and exploratory and confirmatory factor analyses, the study synthesizes findings from several investigations. The creation and confirmation of theories about the influence of perceived risk on user satisfaction and continuing intention are informed by a pilot study involving fifty users of banking chatbots. The key takeaways are as follows-

Privacy Issues & Brand Loyalty- Digital privacy issues have been found to hurt user self-disclosure, according to a recurrent pattern in studies on brand loyalty and privacy.

Trust-Building Strategies- Establishing trust with chatbots in finance industry is a complicated process that calls for a diversified strategy.

Impact of Human-Like Factors- Human like factors, encompassing the chatbot's ability to understand questions and its use of emojis, play a pivotal role in structuring the overall user experience. Incorporating these human-like elements positively impacts user attitudes and satisfaction.

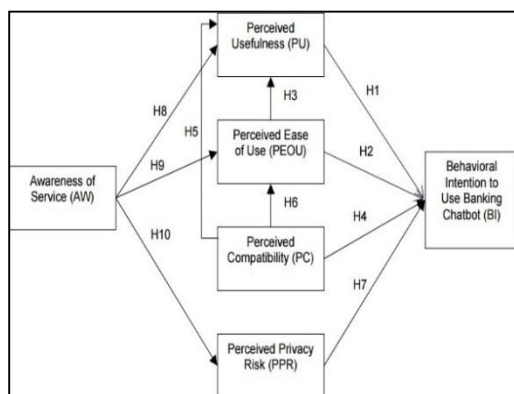


Figure 2. Hypothesized Model

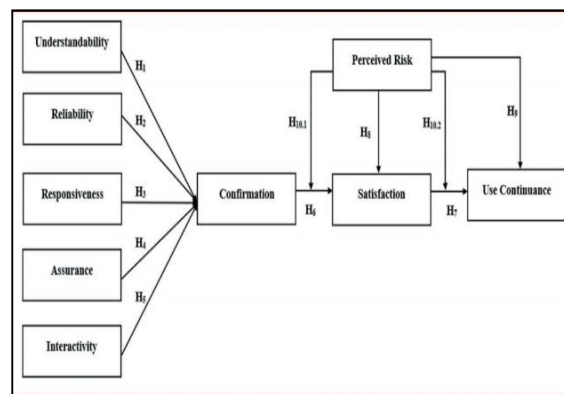


Figure 3. Research Model

Perceived Compatibility and Perceived Usefulness- These two factors are identified as pivotal elements in the adoption of finance chatbot technology. The study provides empirical support for the role of these variables in shaping user perceptions and intentions.

The review extends beyond individual studies, providing a holistic perspective on the factors influencing user attitudes, the role of trust-building strategies, and the adoption of advanced technologies.

Chatbots In Customer Service- The primary objective behind the deployment of chatbots is to increase consumer engagement and happiness. When seen as a multifaceted concept, customer service includes a range of user reactions, such as perceived human likeness, simplicity of use, and misunderstandings. Customer experience-related factors have a significant impact on how users perceive and behave. One important factor that determines whether people will embrace and want to use chatbots is their ease of usage.

Problem 2- Examine the ability of Chatbots to adapt to dynamic and evolving cyber threat landscapes in the banking and finance industry

The research findings cover a wide array of applications and difficulties in the areas of vulnerability identification, chatbot development, and cyber deception. Large Language Models (LLMs) show promise as useful tools for interactive cyber deception and provide a fresh method for creating honeypots.

Regarding vulnerability detection, the study shows how ChatGPT, a generative model, outperforms the best traditional static code analyzer with a success rate of 32%, exhibiting a noteworthy success rate of 62-68% in identifying PHP vulnerabilities.

A rate of 53% is obtained by combining several conventional static code analyzers, indicating possible synergies between generative models and conventional techniques. Nevertheless, ChatGPT displays a significant false positive rate of 91%, which has prompted the investigation of cooperative methods to enhance vulnerability identification. The study's findings provide a thorough examination of the difficulties and uses of generative models in chatbot generation, vulnerability identification, and cyber deception. The subtle observations help to expand our knowledge of the potential and constraints of these technologies, opening new avenues for investigation and useful applications in these dynamic and developing fields.

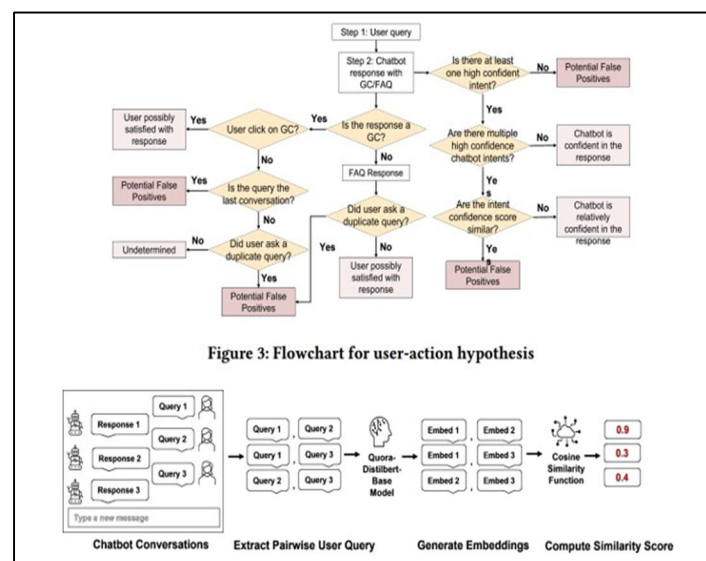


Figure 4. Flowchart for User- Action Hypothesis

Problem 3- Identify and analyze existing and emerging trends, encapsulating newer technologies in the research landscape of Chatbots for Cybersecurity in Banking and Finance

This study explores the profound effects of artificial intelligence (AI) on digital financial inclusion, highlighting the variety of ways in which AI is being used to detect, measure, and manage risks; to address information asymmetry; to provide customer support via chatbots; and to support cybersecurity and fraud detection efforts.

The also study highlights the complex interactions that exist between cybersecurity, digital financial inclusion, and AI. It not only draws attention to the revolutionary potential of AI in the financial sector, but it also offers practical advice for bolstering cybersecurity defences, particularly considering newly developed technologies such as chatbots. The results emphasize how crucial it is to take a thorough and flexible approach to solving changing security issues to ensure the safe and responsible integration of AI in the digital financial ecosystem.

Problem 4- Analyze the challenges, limitations, and opportunities GenAI offers in the cybersecurity space, reflecting different cyber-attacks that can be created and unleashed using chatbots like ChatGPT.

The primary focus of the study in papers is the comprehensive examination of Generative AI (GenAI) in the domains of cybersecurity and privacy. The study aims to shed light on the limitations, challenges, potential risks, and opportunities associated with GenAI.

It outlines open challenges and proposes strategies to fortify cybersecurity alongside the evolution of GenAI technology. These strategies include automated reinforcement learning and meticulous curation of training data to address challenges like hallucinations and adversarial attacks in Large Language Models (LLMs). The study anticipates that as GenAI continues to evolve, these systems will enhance their accuracy and security.

The forward-looking perspective of this study highlights the dynamic nature of GenAI technology and emphasizes the need for proactive measures to navigate emerging threats. It stresses the importance of a responsible and secure integration of these advanced AI systems into our technological landscape.

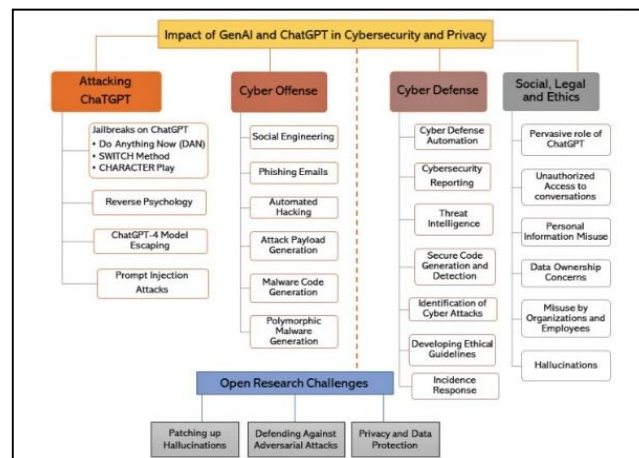


Figure 5. A Roadmap of GenAI and ChatGPT in Cybersecurity and Privacy

V. CONCLUSION

Theoretical Findings-This study explores the elements that impact customer acceptance of banking chatbots in depth, with a particular emphasis on perceptions, future flexibility, and the crucial aspects of human similarity and real-life errors. Investigating these variables helps to clarify important points that influence user acceptability and advance the field's continuing conversation while also illuminating the complexities of how customers engage with this developing technology. The survey also highlights the importance of user trust, noting that consumers are more inclined to accept chatbots as dependable and secure parts of their financial transactions.

Future adaptability is identified as a critical component, acknowledging that the ever-changing terrain of technology progress demands an investigation into users' expectations for the future. For chatbots to be successfully integrated into banking, it becomes necessary to identify and address these real-life problems. The results show that when chatbots demonstrate human-like traits in terms of language competency, conversational aptitude, and general temperament, people are more likely to embrace them.

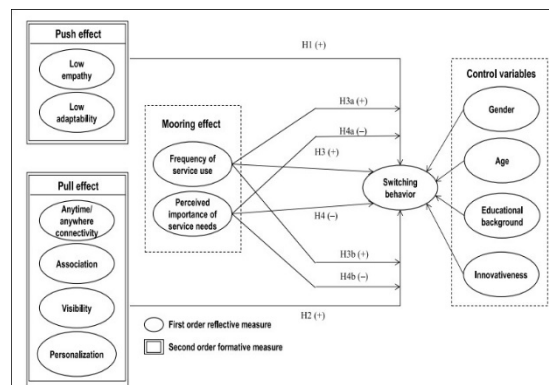


Figure 6. Research Framework of This Study

This SLR explores the dynamics of user self-disclosure in the context of banking chatbots, illuminating the complex interactions between brand trust, emotional considerations, privacy concerns, and service quality. According to the study, there is a complex correlation between user self-disclosure and privacy concerns. Users who are exposed to their favorite banking brand tend to be more cautious when disclosing personal information. As such, it emphasizes how important it is for businesses using chatbots to give privacy concerns priority and develop a thorough architecture of trust that includes brand, cognitive, and emotional trust. The study casts doubt

on the widely held notion that user self-disclosure is solely motivated by brand trust. Rather, it makes the case that a bridge of trust that combines emotional and cognitive aspects is essential. Particularly, emotional elements show up as important contributions to the Technology Acceptance Model's (TAM) ability to anticipate users' intentions to continue using the product in the future. The SLR gives practical insights for a range of businesses by presenting a variety of real-world applications in the areas of chatbot technology, cyber deception, and static code analysis. Chatbot technology develops as a game-changing instrument, opening new services and streamlining consumer banking procedures.

In conclusion, the pervasive influence of Artificial Intelligence (AI) on digital financial inclusion is evident, manifesting through its applications in risk detection, measurement, management, and the mitigation of information asymmetry. The authors advocate for widespread adoption and scaling up of AI usage in the financial sector due to its significant importance. The study recognizes the revolutionary impact of AI and emerging technologies in threat detection and response, highlighting the adoption of Zero Trust Architecture as a critical strategy for enhancing security. The SLR also provides a comprehensive exploration of generative AI technologies, discussing their opportunities, challenges, and broader implications. It emphasizes the need for robust methodologies in distinguishing between human and AI authorship. It also highlights the limitations inherent to GenAI technology, focusing on potential vulnerabilities in models like ChatGPT. Furthermore, the paper explores the dual application of GenAI techniques, defensively and offensively, presenting the nuanced considerations in this domain. They demonstrate common, easily executable cyber-attacks as a practical illustration of the challenges brought by the proliferation of generative AI. Overall, this paper contributes to the ongoing discourse on the responsible development and deployment of generative AI, emphasizing the need for a collective and interdisciplinary effort to navigate the complex landscape of AI technologies, ensuring their positive integration into society while mitigating risks.

Real Life Applications- Beyond theoretical concerns, the research findings have practical applications that provide firms looking to optimize chatbot encounters with useful insights. Businesses can apply the findings of research showing that customers' inclination to use banking chatbots is significantly predicted by perceived utility and perceived compatibility in the real world. One important factor that influences perceived usability, perceived privacy risk, and usage intention is awareness of the service. Contrary to popular belief, behavioral intention is not much influenced by perceived privacy risk or convenience of use. It is imperative to close the gap between theoretical understanding and real-world implementations by providing companies with concrete tactics for enhancing chatbot engagements. In the rapidly changing chatbot ecosystem, the real-world applications—which range from fostering trust to investing in cutting-edge technologies and considering communication nuances—offer organizations a road map for improving user experiences and fostering long-lasting partnerships. This can be documented as-

Notifying Users of Chatbot Limitations- To control user expectations, proactive communication regarding chatbot limitations is crucial. Enterprises ought to furnish precise details regarding the potential and limitations of chatbots, promoting openness and establishing user confidence.

User Experience- Enhancing user experience can be achieved by promoting the use of conversational cues and short sentences. By matching communication methods to user preferences, this useful advice seeks to improve the intuitiveness and interest of encounters.

Purchasing Sophisticated Chatbots for Hard Cases- Businesses are recommended to invest in more sophisticated chatbot technologies because they understand the necessity for sophistication in addressing difficult scenarios. Comprehensive functionalities guarantee that chatbots can efficiently handle complex inquiries, which enhances customer happiness in general.

Examining Other Cues and the Effect of Emojis- It is important to keep in mind how emojis affect user experience. Subsequent investigations on the application of emojis and other indicators in chatbot encounters may yield important information about improving engagement and communication.

Extending Sample Sizes and Analyzing Various Demographics- Future research should concentrate on extending sample sizes and analyzing varying demographics to guarantee the relevance of study results across a range of user groups. This method guarantees a deeper comprehension of how different user segments.

The practical application of this research is crucial in navigating the transformative impact of Artificial Intelligence (AI) on digital financial inclusion and cybersecurity. Recognizing the pervasive influence of AI, financial institutions are urged to adopt and scale up its use for functions ranging from risk detection and management to addressing information asymmetry. AI-driven customer support and chatbots not only enhance user experience but also aid fraud detection and bolster cybersecurity. The study highlights the significant threat cyber risks pose to the stability of the financial system, including financial losses and erosion of customer trust. To counteract these risks, a proactive approach with employee training, continuous monitoring, and

collaboration is deemed essential. The authors advocate for adherence to best practices and the adoption of measures like Zero Trust Architecture to fortify cybersecurity. In the context of chatbots, which offer advantages such as 24/7 availability and cost reduction, the research emphasizes the critical importance of secure communication for data protection.

ChatGPT represents a transformative force with immense potential for innovation in various fields. However, the paper emphasizes the significance of conducting comprehensive research to convey crucial concerns like managing conversations, ensuring equal access, and preserving agency in the context of generative AI. By recognizing the profound influence of gen AI on business, society and government, this study effectively highlights both the opportunities and challenges that come with this technology. One key takeaway is the need for interdisciplinary research and incorporating insights into educational programs to fully comprehend the complex implications of generative AI. Furthermore, the paper sheds light on the significant role that tools like ChatGPT play in shaping cybersecurity landscapes. It particularly emphasizes the potential vulnerabilities of ChatGPT, pointing out the risk of cyber-attacks exploiting the tool to bypass ethical and privacy safeguards. Nevertheless, the dual nature of ChatGPT is acknowledged, highlighting its potential to strengthen cyber defense mechanisms. The discussion extends beyond technical aspects, encompassing social, legal, and ethical considerations associated with generative AI. The papers [1] [2] also provide a comparative analysis of key features between ChatGPT and Google Bard, two influential tools in this domain. Additionally, the conclusion identifies ongoing challenges and research problems in GenAI cybersecurity, focusing the need for continuous exploration and innovation to convey evolving threats and vulnerabilities in this dynamic landscape. Ultimately, the paper encapsulates the multidimensional nature of generative AI and advocates for a holistic approach to understanding, harnessing, and safeguarding against its potential impacts.

REFERENCES

- [1] Olajide Olusegun Adeosun, "The Impact of Artificial Intelligence on Digital Financial Inclusion: A Conceptual Framework," 2018
- [2] Okeoma Onunkaa, Ayoola Maxwell Alabib, Chiedozie Marius Okafor, Anwuli Nkemchor Obiki-Osafialed, Tochukwu Onunkae, Chibuike Daraojimba, "CYBERSECURITY IN U.S. AND NIGERIA BANKING AND FINANCIAL INSTITUTIONS" 2022
- [3] Maanak Gupta, Charankumar Akiri, Kshitiza Aryal, Eli Parker, Lopamudra Praharaj, "From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy" 2023
- [4] Yogesh K. Dwivedi, Nir Kshetri, Laurie Hughes, Emma Louise Slade, Anand Jeyaraj, "Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy" 2023
- [5] Martin Hasal, Khalifa Ahmed Saghair, Jana Nowaková, "Security Aspects in Communication with Chatbots: A Comprehensive Study" 2021
- [6] Nádira Azevedo, Gustavo Aquino, Leonardo Nascimento, Leonardo Camelo, "A Novel Methodology for Developing Troubleshooting" 2023
- [7] Omer Said Ozturk, Emre Ekmekcioglu, Orcun Cetin, Budi Arief, Julio Hernandez Catro, "New Tricks to Old Codes: Can AI Chatbots Replace Static Code" 2019
- [8] Lecia Lim, Samarth Agarwal, Xuejie Zhang, John Jianan Lu, "False Positive Intent Detection Framework for Chatbot Annotation" 2022
- [9] Jarrod Ragsdale, Rajendra V Boppana, "Towards Intelligent and Contextual Interaction in Honeypots: A Simple Language Model Context Honeypot" 2023
- [10] Amalia Zahra, Bhakti Prabandyo Wicaksono, "Design of the use of chatbot as a virtual assistant in banking services in Indonesia" 2021
- [11] Jin Ting Zhang, Chia-Ying Li, "Chatbots or me? Consumers switching between human agents" 2021
- [12] Anine Holtmoen Petersson, Sanchit Pawar, "Investigating the factors of customer experiences using real-life errors and human-likeness in a banking chatbot in Norway" 2019
- [13] Ibolya Vizeli, Zsuzsa Saplacan, Mónika-Anetta, "BANKING WITH A CHATBOT – A STUDY ON TECHNOLOGY ACCEPTANCE" 2021
- [14] Jassim Ahmad Al-Gasawneh, Ahmad Mtair Al-Hawamleh, Almuhammad Alorfi, Ghada Al-Rawashdeh, "The Impact of Influencer Endorsement on Perceived Security and Its Effect on Financial AI Services Adoption: A Moderated Mediation Model" 2022
- [15] Stanley Y. B. Huang, Chih Jen Lee, Shih Chin Lee, "Toward a Unified Theory of Customer Continuance Model for," 2022.
- [16] James Lappeman, Siddeeqah Marlie, Tamryn Johnson, Sloane Poggenpoel, "Trust and digital privacy: The willingness to disclose personal information to banking chatbot services" 2023
- [17] Karine Aoun Barakat, Amal Dabbous, "FACTORS AFFECTING THE SUSTAINED USE OF CHATBOTS: AN ORGANIZATIONAL PERSPECTIVE" 2019

- [18] Monika Anetta Alt, Vizeli Ibolya, “IDENTIFYING RELEVANT SEGMENTS OF POTENTIAL BANKING CHATBOT USERS BASED ON TECHNOLOGY ADOPTION BEHAVIOUR” 2021
- [19] Brighton Nyagadza, Asphat Muposhi, Gideon Mazuruse, Tendai Makoni, Tinashe Chuchu, Eugene T Maziriri, “Anthropomorphic chatbots’ usage intention as an e-banking customer service theory: A Zimbabwean study” 2021
- [20] Sangeeta Mehroliya, Sabburaj Alagarsamy, Vasudevan Moorthy, Jeevananda S, “Will Users Continue Using Banking Chatbots? The Moderating Role of Perceived RiskRole of Perceived Risk” 2021.