

MASTER THESIS

Exploring the Future of
Artificial Intelligence in the
European Banking Industry:
Analyzing Cybersecurity
Risks and Improving
Operational Efficiency



Prepared By:

Ludmila Calcatinci



Supervisor: Dr David Coker



Pathway: Finance and Banking

Master's Degrees by Examination and Dissertation

Declaration Form.

1. This work has not previously been accepted in substance for any degree and is not being concurrently submitted in candidature for any degree.

Signed.....

Date

2. This dissertation is being submitted in partial fulfilment of the requirements for the degree of Master's in Business Administration.

Signed

Date

3. This dissertation is the result of my own independent work/investigation, except where otherwise stated.

Other sources are acknowledged by footnotes giving explicit references.

A bibliography is appended.

Signed candidate: *Ludmila Calcatinci*

Date: 20/10/2023.....

4. I do not give consent for my dissertation, if accepted, to be available for photocopying, inter- library loan, and for deposit in the University's digital repository

Signed (candidate) *Ludmila Calcatinci*

Date.....20/10/2023.....

Supervisor's Declaration.

I am satisfied that this work is the result of the student's own efforts.

Signed: Dave Coker.....

Date: 18/10/23.....

To my parents,

Nicolae and Elena

Pentru părinții mei,

Nicolae și Elena

“Technological innovations will be the heart and blood of the banking industry for many years to come and if big banks do not make the most of it, the new players from Fin-Tech and large technology companies surely will.”

– David M Brear

Acknowledgement

It's been told that it takes approximately 10,000 hours to evolve good at something or 21 days of doing the same thing around and over to complete a habit. After one year of lectures and research on the Financial and Baking landscape, I am happy to present my thesis.

Firstly, I would like to express my profound appreciation to my lecturer and supervisor, Dr. David Coker. His support, insightful feedback, and valuable advice have shaped this dissertation as a diamond. His tolerance and wisdom have made this expedition both demanding and rewarding, and I am genuinely thankful for that.

Equally significant is my enormous appreciation to my husband - Daniel Calcatinci. Without his endless encouragement, understanding, and unyielding support, this work would not have reached realization. He has been my pillar of resilience during the challenging periods of research and writing, furnishing emotional sustenance and unlimited mugs of coffee.

A big thank the University of Wales Trinity Saint David staff, whose input and motivation were priceless. My colleagues and fellow research researchers merit special recognition for their friendship and practical seminars that improved my academic journey.

Ultimately, my sincere gratitude belongs to all my family and friends who stood by me, considered my potential, and delivered much-needed breaks from the rigors of academic life. This journey, with its highs and lows, has been remarkable. The lessons I have learned and the connections I developed during this course will remain with me forever.

Thank you,

A handwritten signature in black ink, reading "Ludmila Calcatinci". The signature is written in a cursive style with a large, stylized 'L' and 'C'.

Abstract

Integrating Artificial Intelligence into the banking and financial sectors indicates a transformative change, encouraging improved efficiencies, unexplored products, and client experiences. Nevertheless, despite the countless possibilities, numerous challenges exist, particularly in risk management. This dissertation delves into the transformative impact of Artificial Intelligence within the European banking sector, highlighting the prospect of improving functional efficiency and managing rising cybersecurity threats with forecasts indicating an exponential boost in the value of AI technologies in the economic environment – from nearly 100 billion U.S. dollars to approximately 2 trillion U.S. dollars by 2030 (Statista,2023). – there is a critical requirement to comprehend AI integration's importance, challenges, and benefits.

The dissertation examination will be through an in-depth case study of the considerable influential banks in Europe; the research delivers an extensive understanding of the functional application and results of AI strategies. Primary data was sourced from the survey "Customer Perspectives on AI-Related Cyber Threats in the Banking System: A Survey on Knowledge, Awareness, and Precautions," targeting level 6 and 7 students at the University of Wales Trinity Saint David(London Campus). Secondary data was collected from rigorous academic literature reviews, industry reports, and pertinent case studies. The research demonstrated various applications of AI in the banking sector, going from client assistance industrialization, fraud detection, and risk assessment to operational optimization. These AI applications can have both promising and adverse outcomes. On one side, they present automation capacities, decreased human mistakes, and more instantaneous client reaction times, facilitating operations and improving efficiency. Contrarily, they bring to light influential challenges, including problems over data privacy, ethical quandaries, and regulatory compliance. As European banks stride toward comprehensive AI adoption, identifying and managing the associated challenges, such as data security, algorithmic bias, regulatory intricacies, and workforce dynamics, evolves essential.

The study underscores financial institutions need to embrace AI's capabilities and navigate its complexities responsibly, ensuring an ethical, compliant, and efficient AI-driven future in the banking sector. Another concern is the students' awareness of cyber threats; the questionnaire revealed that students need digital literature awareness and workshops regarding cyber threats.

Glossary of key terms

Cyber threat	Online attack or harm to digital information and systems.
Digital data	Information that can be held and utilized on computers or electronic devices.
Data Privacy	The protection of confidential information guarantees it's not misapplied or accessed without authorization.
Malicious / Malware Software	Special software designed to harm vulnerabilities in networks or computers.
Privat Information	Personal details or data people control are confidential or not shared openly.
Phishing attacks	Misleading attempts, often through emails, get individuals to transmit private information by acting as somebody reliable.
Cybersecurity	Protect computer methods or data from stealing deterioration, or unauthorized admission.
Operational productivity	The efficiency of delivering goods or services in a company or operation.
Deepfake fraud	Utilization of realistic-looking but faked videotapes or audio, produced employing AI, to mislead, scam, or imitate individuals for hostile intentions.
Regulatory frameworks	Sets of regulations and policies completed by authorities to control and manage explicit actions.
Banking System	Network of economic organizations that supply diverse financial services.
Online Protection	Standards and procedures to protect users from threats and attacks on the internet.
Financial Institutions	Businesses that operate with money as banks, investment firms credit unions and insurance companies.

List of Acronyms

AI	Artificial Intelligence
NLP	Natural language processing
ML	Machine Learning
ESCB	The European System of Central Banks
TEU	Treaty on European Union
ECB	European Central Bank
GDPR	General Data Protection Regulation
EU	European Union
PSD2	Payment Services Directive
MiFID II	The Markets in Financial Instruments Directive II
AISP	Account information service provider
PISP	Payment initiation service provider
AML	Anti-money laundering
DDoS	Distributed Denial of Service
VPN	Virtual Private Networks
2FA	Two-Factor Authentication
GRC	Governance, risk management, and compliance
NLU	Natural language understanding
NLP	Natural language processing
RPA	Robotic Process Automation
ESMA	European Securities and Markets Authority
EUA	European Banking Authority
ICOA	Information Commissioner's Office's
CAMS	Association of Certified Specialists in the Prevention and Combating of Money Laundering

TABLE OF CONTENT

- 0. Index of figures & equations.....11
- 1.Introduction.....12
 - 1.1 Background and Significance.....14
 - 1.2 Research Objectives & Questions.....14
 - 1.3 Scope and Limitations.....16
- 2 Literature Review.....17
 - 2.0 Hypotheses Development 17
 - 2.1 Overview of the European Financial and Banking Area.....18
 - 2.2 Introduction to Artificial Intelligence.....19
 - 2.3 AI Applications in the Financial and Banking Sectors.....21
 - 2.4 Benefits and Limitations of AI Adoption.....21
 - 2.5 Cybersecurity Threats and Data Privacy Concerns.....22
 - 2.6 Regulatory Frameworks and Best Practices for AI Implementation.....24
- 3. Research Methodology.....26
- 4. Current State of AI Adoption in the European Financial and Banking Sectors.....27
 - 4.1 AI Applications in Risk Management.....28
 - 4.2 AI for Fraud Detection and Prevention.....28
 - 4.3 AI in Customer Service and Experience.....29
 - 4.4 AI for Operational Productivity Enhancement.....30
- 5. Case Study: Deutsche Bank - Implementing AI for Operational Productivity and Cybersecurity.....31
 - 5.1 Overview of Deutsche Bank and its AI Initiatives.....31
 - 5.2 AI Applications in Operational Productivity at Deutsche Bank.....31
 - 5.3 Cybersecurity Threats and AI Solutions at Deutsche Bank.....32
 - 5.4 Challenges and Successes in AI Implementation: Lessons from Deutsche Bank.....32
 - 5.5 Case Study: HSBC Bank - Ayasdi: AI for Anti-Money Laundering.....34
 - 5.6 Overview of HSBC Bank and its AI Initiatives.....34
 - 5.7 Ayasdi's AI Solution for Anti-Money Laundering.....34
 - 5.8 Benefits and Successes of Ayasdi's AI Solution at HSBC Bank.....35
 - 5.9 Challenges and Lessons Learned from AI Implementation at HSBC Bank.....35
- 6. Cybersecurity Threats and Data Privacy Challenges in the European Financial and Banking Sector...36
 - 6.1 Overview of Cybersecurity Threats in the Financial and Banking Sectors.....36
- 7. Mitigating Cybersecurity Threats: Best Practices and Solutions.....37

8.The Cyber Threat of AI in the Banking System: Considerations from the Customer's Perspective.....38

8.1 Introduction to AI-related Cyber Threats in the Banking System.....38

8.2 Phishing Attacks: Exploiting AI for Social Engineering.....39

8.3 Deepfake Fraud: Impersonation and Manipulation with AI-generated Content.....40

8.4 Being Wary of Suspicious Communications.....42

8.5 Banks' Efforts in Ensuring Security and Privacy.....43

9. Regulatory Frameworks and Ethical Considerations in AI Implementation.....44

9.1 Overview of AI-related Regulations in the European Financial and Banking Sectors.....44

10. Prospects of AI in the European Financial and Banking Area.....46

10.1 Emerging Trends and Technologies in AI.....46

11. Conclusion.....47

11.1 Recommendations for Successful AI Integration.....48

12. Summary of Findings.....49

12.1 Contributions to Knowledge.....50

13. References.....51

14.Appendix.....60

0.2 Index of figures & equation

Chart No 1.....13

Chart No 2.....19

Figure No 1.....20

Equation No 1.....38

Diagram No 1.....38

Diagram No 2.....39

Diagram No 3.....41

Diagram No 4.....42

Table No 1.....39

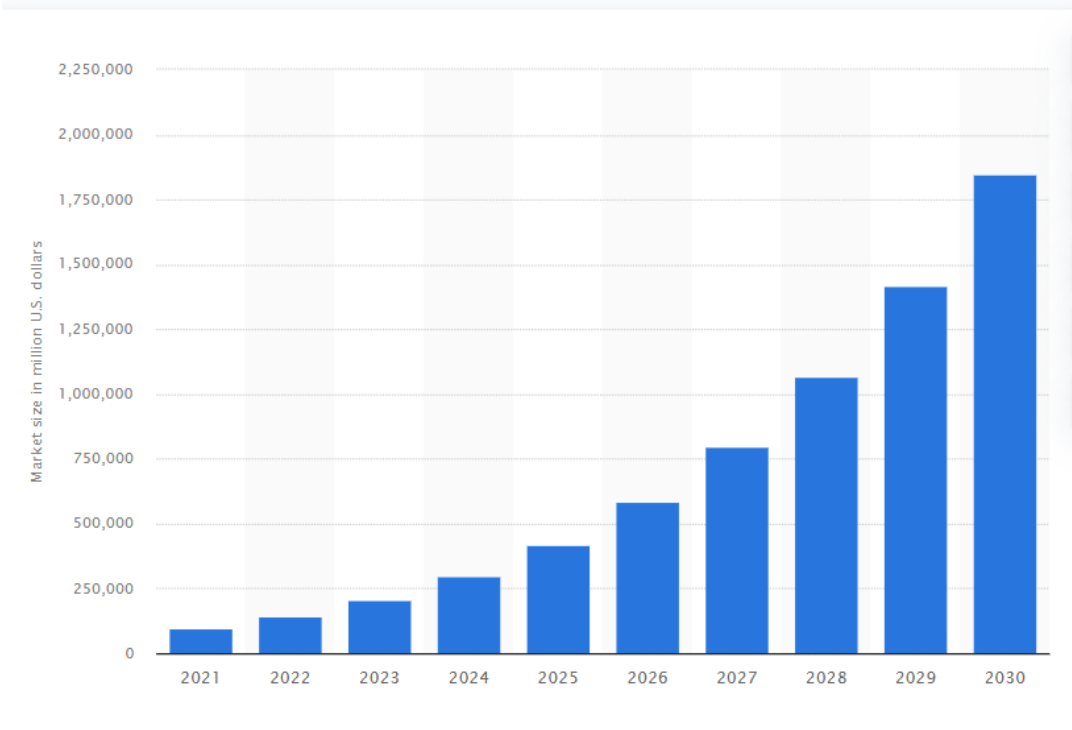
1.Introduction

The quick improvement of Artificial Intelligence (AI) technology has transmitted meaningful changes in diverse sectors, including the financial and banking industries. According to Thormundsson (2023), the value of nearly 100 billion U.S. dollars is expected to grow twentyfold by 2030, up to almost 2 trillion U.S. dollars by the end of the decade (Shetty,2022). AI offers unparalleled prospects to improve operational efficiency, enhance customer experience, and drive innovation in financial services.

Nevertheless, alongside its advantages, AI also presents new challenges and possible risks, especially cybersecurity. This dissertation analyses how the European banking sector can effectively utilize AI to improve operational efficiency and mitigate cybersecurity risks using a case study of the most predominant banks in the system. The focus is on comprehending the potential advantages, challenges, and importance of incorporating AI technologies within banking procedures. By exploring the utilization of Artificial intelligence in the European banking sector, this research aspires to understand the practical performance of AI strategies while managing potential cybersecurity circumstances.

The dissertation will focus on investigating diverse applications of AI in banking, including customer assistance automation, fraud detection, risk assessment, and operational optimization. Robotic Process Automation (RPA) tools can help businesses improve the efficiency and effectiveness of their operations faster and at a lower cost than other automation approaches(Deloitte United Kingdom, 2018). Another tool that helps businesses improve their operations' efficiency and efficacy quicker and at a lower expense than other automation approaches. AI and ML encompass more "thinking" and "learning," respectively. It trains algorithms using data so that the software can perform tasks quicker and more efficiently(IBM,2023).

According to Hertz(2023), these applications enable banks to automate routine tasks, minimize human error, and provide faster, more accurate responses to customer queries. These applications can simplify processes, improve decision-making, and enhance prevalent efficiency within financial institutions. Regardless, they also introduce influential concerns concerning data privacy, ethical implications, and regulatory compliance. The primary data will be extracted from the author's questionnaire Customer Perspectives on AI-Related Cyber Threats in the Banking System: A Survey on Knowledge, Awareness, and Precautions, which will be conducted at the University of Wales Trinity Saint David for level 6&7 students. For the secondary data, academic literature reviews, industry reports, and case analyses will be analyzed to achieve the research objective. The study will delve into the contemporary landscape of AI adoption in the European banking sector, investigating the approaches employed by leading financial institutions and determining the fundamental elements contributing to successful AI performance. Further, the research will address the challenges associated with AI adoption in the banking sector, such as data privacy and security algorithmic bias, such as impact assessments, audit standards (Centre for Data Ethics and Innovation 2020),regulatory compliance, and the potential impact on workforce dynamics. Understanding these challenges is crucial for financial institutions to navigate the complexities of AI adoption and ensure the responsible and effective use of AI technologies.



Chart, no 1. Tormund's, B. (2023). *Artificial Intelligence market size2030*.

1.1 Background and Significance

The European financial and banking industry functions within a diligent atmosphere distinguished by quick technological advances, developing customer anticipations, and modifying regulatory frameworks. Regardless of the potential to reshape the financial environment, Artificial intelligence can act as a disruptive force. By leveraging the techniques to automate manual procedures, make data-driven judgments in real-time and derive actionable insights from vast amounts of data, the financial institution can leverage AI algorithms as a risk factor because of the potential susceptibility to errors (Artificial Intelligence in Financial Services in Europe Report,2022). Nevertheless, implementing AI also escalates problematic cybersecurity issues for financial institutions. The banks are accountable for protecting consumer data, providing secure financial transactions, and safeguarding against antagonistic steps.

To provide resilience and implement practical AI tools that can address cyber-attacks, privacy concerns, and data breaches, it is essential to understand how effective those tools can be and not underestimate the customer's support to prevent those attacks by educating them to react to spam or other risks. Besides, operational productivity is a significant priority for financial institutions that maintain competitive advantage. Using the potential of AI can augment human abilities, optimize resource distribution, and propose the possibility of facilitating operations.

1.2 Research Objectives and Questions

This research aims to analyze how the banking sector in Europe can effectively utilize Artificial Intelligence to boost the efficiency of operations and mitigate the cyber threat. As we transition to a digital economy, cybersecurity in banking is becoming a serious concern. Utilizing methods and procedures created to safeguard the data is essential for a successful digital revolution(Naz, 2023).

The study explores the potential benefits, challenges, and implications of integrating AI technologies within banking operations. More precisely, by scrutinizing the utilization of AI in the European banking sector, the research aspires to deliver insights into the effective implementation of AI strategies while addressing potential cybersecurity concerns.

Given the complexity of the case under investigation, the study aim has diverged into the following objectives:

- Determinate the landscape of AI adoption in the European banking sector, including AI technologies' applications and use cases in various banking operations.
- Assess the potential benefits of AI utilization in improving operational efficiency, enhancing customer experience, and driving innovation in financial services.
- To examine the challenges and risks associated with AI adoption in the banking sector, such as data privacy and security concerns, algorithmic bias, regulatory compliance, and the impact on workforce dynamics.
- To create a study at the University of Wales Trinity Saint David to evaluate the students' awareness of Cyber threats in the daily use of devices by providing a questionnaire.

The central questions is : How can the European financial and banking sector productively leverage the prospect of AI to improve operational efficiency while managing cybersecurity threats in the condition of the cyber danger of Artificial intelligence in the banking system, evaluating customers' perspectives?

- How can economic organizations enhance customer collaboration to handle cyber threats and help control financial crime?
- What actions are financial institutions carrying to provide security and privacy in the face of AI-related cyber dangers, and how are they adjusting their systems to protect customers?
- How aware are the customers- students at University of Wales Trinity Saint David London campus of cyber threat?

According to the International Monetary Fund (2021), Cyber threats to the financial system are growing, and by achieving these research objectives, the study aims to contribute to the existing knowledge base and provide valuable insights for financial institutions in the European banking sector. Banking cyber security is an issue that cannot be bargained with. Hackers are more likely to target the banking sector as digitalization advances(Naz,2023). The findings will inform decision-making processes regarding the adoption and integration of AI technologies, helping organizations harness the potential of AI to improve operational efficiency while maintaining robust cybersecurity practices.

1.3 Scope and Limitations

The banking industry has long been aware of cyberattack threats, but it may be more vulnerable now than ever (Sayegh,2023).This dissertation focuses on improving operational efficiency and mitigating cybersecurity risks. The research will investigate diverse applications of AI in the banking sector, such as customer service automation, fraud detection, risk assessment, and operational optimization (Haricharan,2023). It will explore the benefits and challenges of implementing AI technologies in banking operations. The first limit is that the research focuses on specific AI applications in banking: customer service automation, fraud detection, risk assessment, and operational optimization. Further possible uses of AI, such as AI in asset advisory or credit scoring, need to be examined.

The study will consider relevant academic literature, industry reports, and case studies to understand the current AI landscape in the European banking sector to achieve the objective. The analysis is embedded in current issues, citing literature as current as 2023.

Consequently, historical trajectories or evolutions of AI in banking before recent years could be more superficial. The research will also explore the regulatory frameworks and ethical concerns associated with adoption of AI in banking to assure compliance and protect customer privacy.Nevertheless, there are specific limitations to consider in this dissertation:

Access to Data: Data availability for analysis is limited due to privacy and confidentiality considerations. According to Yoskowitz(2023), data has never been more sensitive, and now more people can see it. Access to data from financial institutions is restricted, affecting the profundity of the study and the ability to draw definite conclusions.

Time Constraints: Conducting a comprehensive examination of the entire European banking sector may be challenging within the scope of the dissertation. The time available to study the research problem and to measure change over time might be constrained by such practical issues (Wordvice,2023).Therefore, the research may concentrate on specific case studies or select a representative sample of banks for analysis.

Rapidly Evolving Landscape: The future of *AI is constantly* in flux. *AI is changing* nearly every industry and will impact society in ways we are just beginning to understand (Thomas,2023). AI in banking is rapidly evolving. New technologies and techniques may emerge during the research. It is important to recognize that the findings may reflect the state of AI adoption at an exact time and need to be validated and updated.

External Factors: The efficacy of AI in the European banking sector may be affected by external elements such as market dynamics, regulatory changes, or geopolitical events. The unforeseen twists in *AI* development may affect the research findings (GSAM website,n.d.). While the research will endeavor to evaluate these factors, their impact on AI adoption and implementation may vary over. Regardless of these constraints, the paper aspires to deliver a practical understanding of how the European banking sector can effectively leverage AI to enhance operational efficiency and manage cybersecurity threats. The examination will contribute to the understanding base by determining the most suitable approaches, challenges, and possible resolutions for successful AI adoption in the banking industry.

2. Literature Review

Over the past years, significant attention has been garnered in Europe on the performance of AI. In the following section, the customer will examine the literature review concentrating on the key studies and research findings on how AI can effectively enhance operational efficiency while addressing cybersecurity threats in these sectors.

2.0 Hypotheses Development

The first hypothesis is that Implementing AI technologies in European banking organizations corresponds to an expansion in registered AI-centric cybersecurity threats.

The second hypothesis is that Financial institutions that prioritize behavior-based AI authentication and training to customers procedures experience fewer AI-induced security breaches than classic cybersecurity measures.

The third hypothesis is that Implementing AI technologies in European banking institutions equals an increased recorded AI cybersecurity threats.

2.1 Overview of the European Financial and Banking Area

The European financial and banking structure incorporates domestic and international institutions, leading to cooperation between central banks in the Eurozone; this is referred to as the Euro system (European-union website, n.d.). The major financial centers are in London, Zurich, Frankfurt and Paris, hubs for banking and economic activities. They serve as centers house for numerous investment firms, stock exchanges, and global banks, contributing to the attractiveness and competitiveness of the European financial market.

Euro System operates under a comprehensive regulatory framework to ensure transparency, stability and investor protection. The European System of Central Banks (ESCB) established under the Treaty on European Union (TEU) is made up of the European Central Bank (ECB) and the national central banks of all the Member States of the European Union (Banco de Espana, n.d.). The regulator supervises and positions the monetary policy to maintain financial stability. Being home to significant players starting with financial institutions, regional and global banks, some of the biggest players are HSBC Holdings PLC, BNP Paribas, Banco Santander SA, and Deutsche Bank AG (S&P Global, 2023). These banks perform across numerous countries, providing financial services to individuals, companies, and institutional consumers.

The European economic and banking zone is a complex and interconnected ecosystem. In the European region, financial stability vulnerabilities remain elevated in the context of unexpected stress in the banking sectors of some mature economies (Bank, E.C., 2023).

The recent financial distress experienced by multiple regional banks in the United States and the acquisition of a Swiss bank has initiated an elevated grade of reexamination concerning the capacity to which banks are exposed to long-term fixed-income securities. *According to Mara Monti (2023), “the European banking sector is in a far stronger position than it was during the global financial crisis 2008, and the banking turmoil has encouraged E.U. leaders to push for economic integration”.*

In the Chart NO 2 (please see below) the Macro-financial circumstances have enhanced narrowly since the last Financial Stability Review (Chart a), according to post-pandemic recovery, decreased global supply chain disturbances, and lower energy prices. However, anticipations continue due to downside threats to development and persistent inflationary tensions. Financial stress indicators (Chart b) have improved likewise, especially in the banking sectors of certain grown economies, but remain below pandemic and war-related events.

a) 2023 real GDP growth and inflation forecasts for the euro area and the United States

(10 Jan. 2022-23 May 2023; percentages)

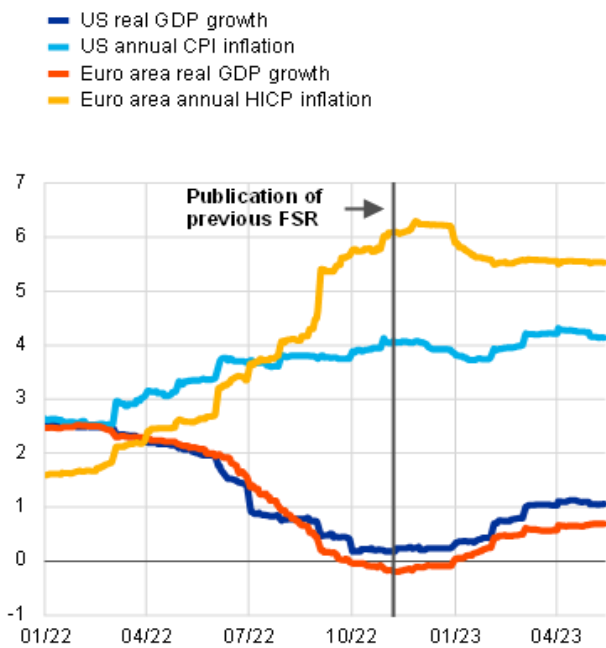
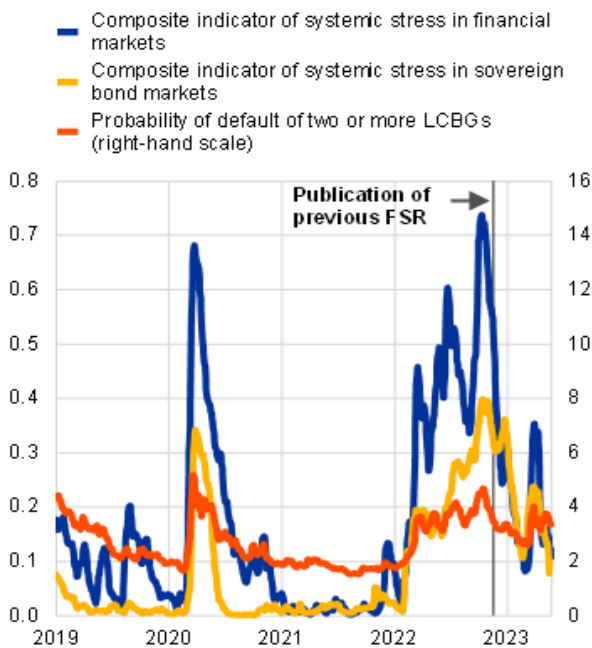


Chart No. 2. Real GDP growth and inflation forecast in Eurozone and US.

b) Near-term financial stress indicators for banks, financial markets and sovereigns

(1 Jan. 2019-23 May 2023; probability of default, percentages)



2.2 Introduction to Artificial Intelligence

Intending to institute " thinking machines" and to solve complex math's problems in 1950, modern Artificial intelligence was initiated. In figure number three is illustrated the History map of Artificial Intelligence. In 1642, the French mathematician and physicist Blaise Pascal developed one of the earliest mechanical calculators -the Pascaline. This device could execute superficial arithmetic operations, designating a significant leap in automating mathematical studies.

In 1837 Charles Babbage - "father of the computer," developed the concept for the Analytical Engine, a general-purpose mechanical-automatical computer. His Engine was created to utilise perforated cards, a process encouraged by the Jacquard loom, and would be qualified for maintaining memory and performing arithmetic processes.

In 1943 the foundation for cybernetics was introduced and would later influence the development of artificial neural networks in AI by McCulloch and Walter Pitts.

In 1950, Alan Turing suggested the idea of a universal machine known today as the Turning machine—the criterion for deciding whether a device can demonstrate human-like intelligence.

In 1955 John McCarthy, Marvin Minsky, Nathaniel Rochester, and Claude Shannon proposed a project now identified as the conception of AI as an academic field. The idea of "Artificial Intelligence" was coined, and the foundational assignment aimed to examine if every aspect of learning or any further intelligence element could be so strictly defined that a device could imitate it.

In 1965, ELIZA, NLP Program, was one of the earliest natural language processing computer programs. The program ELIZA was one of the first chatbots(MIT,2022).

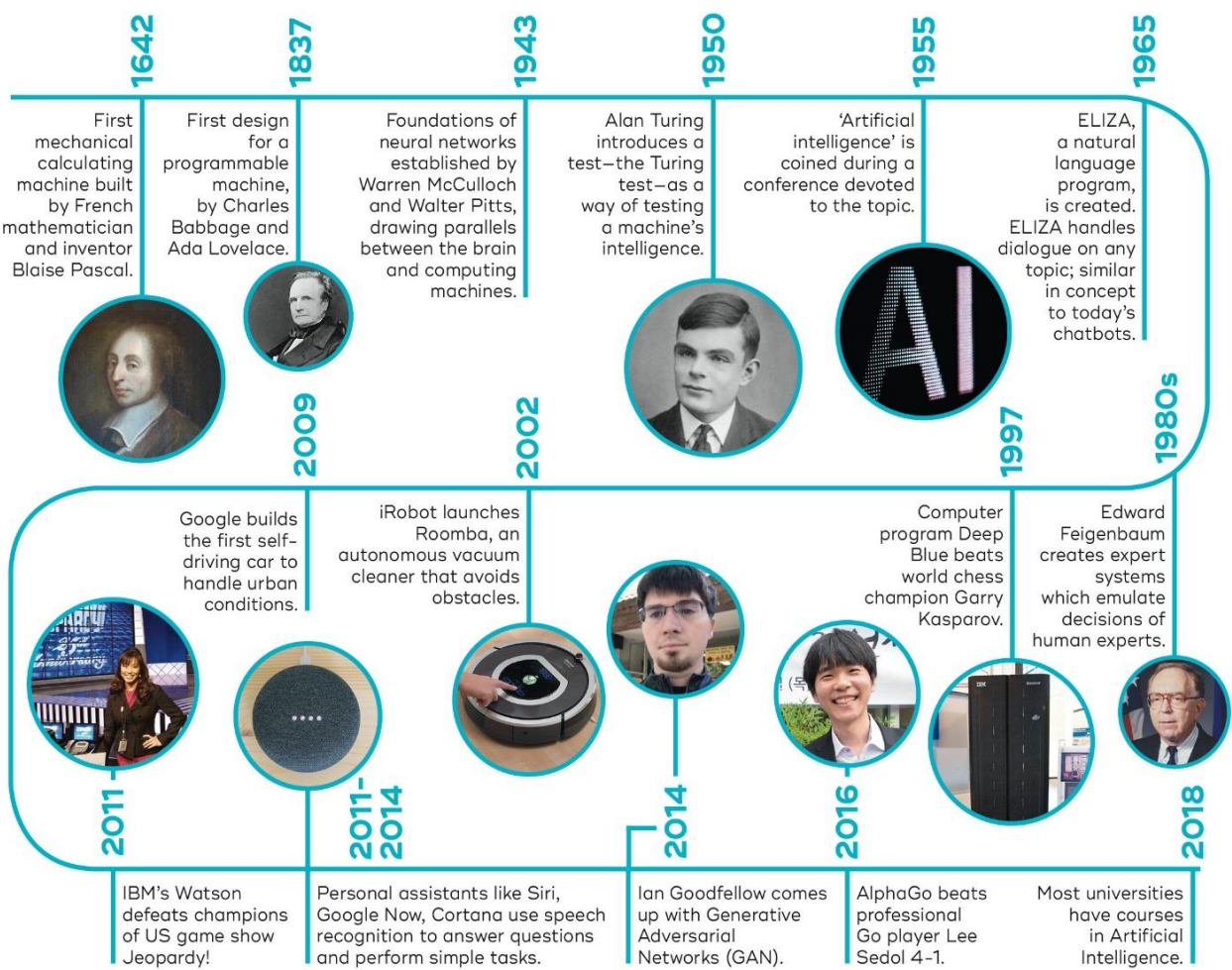


Figure No 1.History of Artificial Intelligence(Queensland Brain Institute,2019).

In 1980, Edward Feigenbaum developed the DENDRAL program, a chemical analysis expert system.

In 1997, Deep Blue showcased the immense possibility of AI in distinct disciplines, meaning a device's ability to exceed human expertise under challenging tasks.

In 2002, Roomba launched iRobot, an independent robotic vacuum cleaner. This is the first AI-powered robot.Starting with 2009 is a boom in AI theologies, Google's Self-driving Car (2009), IBM's Watson (2011), Personal Assistants (2011-2014), Generative Adversarial Networks (GANs) in 2014,I system AlphaGo defeated Lee Sedol. AI has attained considerable engagement in the financial and banking sectors because it can revolutionize processes, enhance decision-making, and navigate invention. A subset of AI is machine learning, essential in financial applications. According to IMB(2023), *Machine learning is a branch of artificial intelligence and computer science that focuses on using data and algorithms to imitate how humans learn, gradually improving its accuracy.*

Another AI language procedure financial institutions employ is Natural Language Processing (NLP), which enables machines to comprehend and analyze human language, permitting computerized analysis of customer queries, sentiment analysis, and text summarization. NLP draws from many disciplines, including computer science and computational linguistics, to fill the gap between human communication and computer understanding (Analytics Software & Solutions,2019).

2.3 AI Applications in the Financial and Banking Sectors

Oliver Wyman (2019), in the article *Artificial Intelligence Applications In Financial Services*, "describes AI as a "powerful tool that is already widely deployed in financial services ". According to the study by the companies SAS, KPMG and the Association of Certified Specialists in the Prevention and Combating of Money Laundering (ACAMS), in the period after the pandemic in 2022, the rate of banking fraud and crime increased. Evidence shows that the surge in online transactions made do diligence more complex and increased money laundering risks (Dupire, 2022). A third of the financial institutions accelerated the integration process of Artificial Intelligence and Machine Learning technologies for more effective crime detection.

2.4 Benefits and Limitations of AI Adoption

Enforcing AI also has substances for the competitive landscape in the financial sector. It may lead to behavioral transformations and give specific institutions a comparative advantage via AI, at least until general implementation appears. Further, consumer protection and personal data processing issues may arise due to AI adoption. According to Tobin(2023), discriminatory outcomes resulting from AI use may contravene the protections set out in the Equality Act 2010.

Given these concerns, there are different opinions among financial regulatory and supervisory authorities concerning the extent to which AI should be incorporated into banking regulation and supervision. Consequently, achieving harmonization and balance between AI and human intervention is desirable. Companies benefit from optimizing collaboration between humans and artificial intelligence (Wilson and Daugherty, 2019).Hitting the right balance would permit leveraging AI's benefits while mitigating potential risks and ensuring effective regulatory oversight.

2.5 Cybersecurity Threats and Data Privacy Concerns

The financial sector performs in a highly interconnected and data-driven atmosphere, causing it a prime target for cybercriminals seeking to manipulate vulnerabilities and regularly infiltrating and *using data* to impersonate individuals *and gain access to sensitive information* (Harrison, 2021).

Financial organisations increasingly embrace Artificial Intelligence technologies, and the possible threats associated with cybersecurity dangers and data privacy matters become even more critical.

This section examines the evolving nature of cybersecurity threats and highlights the vital importance of data privacy and the multifaceted challenges faced by the financial sector; in the past years, the financial industry has detected a wave of sophisticated cybersecurity dangers that aspire to compromise financial data's integrity, confidentiality and availability.

Hostile actors use various methods, such as progressive continuous threats, ransomware attacks, *denial of service attacks*, *system exploits*, and *malware*(Milne, 2021), to exploit vulnerabilities in financial systems. These weaknesses pose intense risks to financial institutions, leading to economic failures, reputational harm, regulatory non-compliance, and compromised client confidence. Financial institutions must stay vigilant against arising dangers, continually revising their security mechanisms to manage the growing nature of cyber attacks. According to the GOV.UK(n.d) to build a *solid* organisational *cyber security* resilience foundation. A complete cybersecurity framework containing robust network security, encryption, access controls, and incident response mechanisms is essential to mitigating these threats. Nevertheless, collecting, holding, and processing such data raise privacy considerations regarding the unauthorized access, misuse, or mishandling of *particularly sensitive information*(Information Commissioner's Office, 2018).

In the European Union, the financial institution must adhere to the General Data Protection Regulation (GDPR) to guarantee the privacy and confidentiality of customer data.

Enforcing data anonymization, encryption, and stringent access authorities can help protect against possible data breaches and unauthorized exposures.

While AI presents considerable advantages, its adoption in the financial sector brings new risks and challenges that must be addressed to ensure financial stability(Boukherouaa et al., 2021).The reliance on AI systems is increasing, making potential attack surfaces for cybercriminals to control. Antagonistic attacks, wherein attackers manipulate AI algorithms by introducing subtle modifications to input data, can trick AI systems and compromise their decision-making procedures.

However, when trained on biased or preliminary datasets, AI models can be sensitive to bias. This bias can include negative importance in financial decision-making procedures, conducting unequal treatment of clients or incorrect risk assessments. Financial institutions must be mindful of these exposures and enforce criteria to address them, such as rigorous testing, auditing, and ongoing monitoring of AI models.

With more than 30 years of experience in cyber threat, the Intrust IT cybersecurity consultant Dave Hatter said: "As more of our physical world is connected to and controlled by the virtual world, and more of our business and personal information goes digital, the risks become increasingly daunting. While managing cybersecurity risk has never been more important, it has never been more difficult (Knowles,2021)." Financial institutions must implementable a visionary and multi-layered technique to mitigate cybersecurity dangers and manage data privacy matters.

This applies to implementing technical standards, worker training, and strong procedures and practices. Technological measures include deploying cutting-edge threat detection, intrusion prevention, and endpoint safeguards. Routine vulnerability examinations and penetration testing can decide probable weaknesses and allow convenient remediation. Additionally, employee training agendas concentrating on cybersecurity awareness, phishing prevention, and protected data handling are essential for creating a safety culture within the association. For a safety culture to be thriving, it needs to be led from the top—that is, safety culture needs to be embraced and practised by the CEO and senior managers (Workplace Health and Safety Queensland,2013)Financial organizations must cooperate with industry associates, share threat intelligence, and contend with regulatory bodies to remain current on the most delinquent cybersecurity directions and best procedures. The financial sector can support its protection against cyber threats and safeguard sensitive financial data by promoting a collaborative effort. In overview, the financial industry meets ever-evolving cybersecurity threats and data privacy situations aggravated by the adoption of AI.

Financial institutions must prioritize robust cybersecurity standards, attach to data protection ordinances, address exposures connected with AI adoption, and execute a multifaceted strategy to mitigate these threats effectively. The financial sector can safeguard its operations, customer data, and stakeholders' trust and confidence in an increasingly digital geography.

2.6 Regulatory Frameworks and Best Practices for AI Implementation

The EU's approach to artificial intelligence centres on excellence and trust, aiming to boost research and industrial capacity while ensuring safety and fundamental rights (European Commission, 2023). The fast promotion of Artificial Intelligence (AI) technologies has stimulated European regulatory bodies to design frameworks to govern AI's reliable and ethical performance in the financial and banking sector.

These frameworks aspire to balance facilitating safeguarding and innovation of the financial system's resilience, integrity, and safety. This part of the dissertation concerns the regulatory geography in Europe and emphasizes the most advantageous techniques for AI performance in the financial and banking system.

In Europe, regulatory bodies have identified the necessity to designate precise policies and frameworks to manage the challenges and threats associated with AI adoption in the financial sector. The European Union has brought a visionary process, developing regulations and initiatives to ensure AI's ethical and responsible use. The General Data Protection Regulation (GDPR), the rectified Payment Services Directive (PSD2), in other words, the PSD2 supports innovation and competition in retail payments and enhances the security of payment transactions and the protection of consumer data (European Central Bank, 2019).

The Markets in Financial Instruments Directive II (MiFID II) are some of the key regulations that have implications for AI implementation. MiFID II was lauded as the accelerator of digitalisation in the financial services industry. New technology would be adopted to help banks and other financial firms comply with the regulations (Holmes, 2017). The General Data Protection Regulation 2018 sets out regulations and conditions for collecting, processing and storing personal data. It gives people more control over their data and sets stringent responsibilities on institutions to guard personal information. The organisations have obligations under UK data protection law to handle the data carefully and by the Information Commissioner's Office's (ICO) guidance (Finextra Research, 2023). Financial institutions need to provide adherence to GDPR when leveraging AI technologies to process customer data. PSD2's purpose is to enhance competition and invention in demand for payment services while delivering customer data security. Financial institutions must have access to client account information from licensed third-party providers, known as an account information service provider (AISP) lets you see data from all your selected accounts in one place and can analyse your spending. Moreover, a payment initiation service provider (PISP) enables the customer to pay companies directly from their bank account rather than using their debit or credit card through a third-party, such as Visa or MasterCard (FCA, 2023).

The usage of AI in supplying these services must be aligned with the regulatory obligations represented in PSD2. In 2018, MiFID II introduced controls on investment services and activities in the EU. It sets transparency requirements for financial institutions to cover investors' interests. The institutions must ensure subordination with MiFID II regulations when AI algorithms are utilised in investment decision-making, including disclosing algorithmic trading actions and controlling market abuse. Financial institutions should consider implementing the following best practices in order to assure compliance and ethical AI techniques in the economic and banking system:

1. **Governance and Risk Management:** *AI governance* frameworks could help organizations learn, govern, monitor, and mature AI adoption (University of Pennsylvania, n.d.). A dedicated governance framework for AI that contains senior management direction, precise roles and responsibilities, and strong risk management approaches. Periodic risk examinations and audits can assist in identifying and mitigating potential risks associated with AI implementation
2. **Data Privacy and Security:** Organisations must comply with data protection regulations like GDPR by enforcing solid data privacy and security standards. This includes encryption, key controls, and standard data protection impact assessments. While the ethical and security risks posed by AI are significant, they can be effectively managed by proactive boards and management. Banks must ensure this is done as AI's rapid uptake and expansion continues. (Atkins, 2021).
3. **Algorithmic Transparency and Explainability:** According to HSBC's published article by the Head of Artificial Intelligence Ash Booth, "Explainable AI is just one part of creating the transparency and interpretability that will allow for the same accountability when an algorithm makes the decision"—enhancing transparency by embracing explicable AI techniques that indeed explain how AI algorithms reach judgments. This promotes confidence and helps regulators and clients to comprehend the reason behind AI-driven products.
4. **Human Oversight and Accountability:** Human oversight helps ensure that an AI system does not undermine human autonomy or cause other adverse effects (Weiser, 2019). They are maintaining human management and accountability in AI procedures to guarantee that findings made by AI are appropriately observed and examined. Human experts must be able to intercede, correct mistakes, and manage unintentional effects.
5. **Collaboration and Industry Standards:** Banks are already strengthening customer relationships and lowering costs by using *artificial intelligence* to guide customer engagement (McKinsey, 2021). Cooperating with regulatory bodies, industry peers and professional institutions to intercommunicate best approaches, design industry standards, and base common frameworks for AI commission. This promotes knowledge sharing and encourages constant ethical procedures across the financial and banking sector.

Banking is at a pivotal moment, technology disruption and consumer shifts are laying the basis for a new S-curve for banking business models, and the COVID-19 pandemic has accelerated these trends (McKinsey, 2021). In closing, regulatory frameworks and best methods are essential in shaping AI's accountable and ethical performance in the financial and banking system. European regulatory bodies have determined the demand for vigorous laws, such as GDPR, PSD2, and MiFID II, to manage data privacy, security, and transparency considerations. Financial institutions need to follow these ordinances while enforcing ethical approaches, including algorithmic transparency, justice, and human oversight. By adopting these precepts and rules, financial professionals can harness the advantages of AI while securing the integrity, resilience, and reliability of the monetary and banking system in Europe.

3. Methodology

This study will utilize a mixed-methods research design, incorporating qualitative and quantitative techniques. The qualitative aspect will involve examining online data on websites, articles, case studies, reports, and other trustable sources associated with cyber threats, client perceptions, and the opening of AI in the financial sector. This will provide an exhaustive interpretation of the present knowledge and directions. The evidence obtained will enable the author to address the research problem as unambiguously as possible effectively (Sacred Heart University Library, 2020).

An anonymous questionnaire will be developed to collect primary data on client perceptions and perspectives towards cyber threats and the introduction of AI in the financial sector. The questionnaire will be administered and sent via student email and in student's group to a focus group of students at the University of Wales Trinity Saint David (UWTSD) London Campus who are enrolled in Level 6 and Level 7 programs of study. Targeting students in these classes will furnish a more critical and knowledgeable philosophy due to their advanced knowledge and understanding of the subject matter (Please see the appendix No 1.). The data accumulated via the questionnaire will be examined by operating statistical software (SPSS). Defining statistics will outline and summarize data and participants' answers.

4. Current State of AI Adoption in the European Financial and Banking Sectors

A study by the World Economic Forum reveals that AI adoption in the financial services industry is already significant, with 85 per cent of organizations claiming to currently use AI in some capacity (Financial IT,2023). The European financial and banking sectors are at the vanguard of assuming Artificial Intelligence Technologies, pushed by the potential to revolutionize corporation processes and improve decision-making strategies. AI's capacity to interpret extensive quantities of data, recognize ways, and create forecasts has caused considerable attraction among financial organizations. This section provides:

An exhaustive examination of the present condition of AI adoption in Europe Zone.

- Concentrating on critical applications in risk management.
- Fraud detection and precluding.
- Client service and experience.
- Operating productivity enhancement.

4.1 AI Applications in Risk Management

Artificial Intelligence (AI) and Machine Learning (ML) techniques are creating waves within the financial services landscape (KPMG, 2021). AI applications in threat oversight have garnered significant engagement within the European financial and banking sectors. AI technologies such as Machine Learning (ML) algorithms and predictive analytics encourage financial organizations to enhance risk assessment models, optimize capital allowance, and improve prevalent risk management systems. AI-powered threat standards leverage recorded data, market trends, supplier performance issues, and market volatility (Kushner, 2023). Interpreting complicated data collections and performing strategy analysis, AI algorithms can deliver real-time threat understandings, assisting in determining occurring threats and designing practical risk mitigation methods.

These applications have advantages in credit risk assessment, portfolio optimization stress-testing scenarios and lowering the possibility of making erroneous judgments and conclusions (Kushner, 2023). Likewise, AI improves fraud detection and precluding mechanisms, permitting financial institutions to bypass fraudulent actions and protect their assets. Machine Learning algorithms can analyze large volumes of transactional data, detecting potential fraudulent activities and flagging them for further investigation (Jeffers, 2023). AI-driven fraud detection systems continuously learn from new data and adapt to evolving fraud patterns; as AI systems process more data, they improve their accuracy in detecting fraudulent practices, reducing false positives and increasing true (Basnet, 2023). The risk powered by models leverage documented data, market trends, and economic indicators to determine ways and consider potential risks. AI algorithms can deliver real-time risk understandings by researching complex data collections, performing strategy investigations, selecting emerging hazards, and developing effective risk mitigation strategies. These applications are advantageous in credit risk assessment, portfolio optimization, and stress-testing scenarios.

4.2 AI for Fraud Detection and Prevention

The terms AI, and machine learning is often used interchangeably. However, while every form of machine learning counts as AI, not every AI uses machine learning (Tanant, 2018).

AI's fraud detection and prevention systems leverage progressive techniques such as abnormality detection, network investigation, and behavioural analytics to determine suspect actions. By examining transactional data, customer behaviour, and historical designs, these methods can notice complicated fraud practices and variations from typical behaviour. AI allows financial institutions to react swiftly to fraudulent actions, underestimating possible economic defeats and safeguarding customer interests.

Likewise, AI algorithms can improve anti-money laundering actions by noticing uncommon transaction practices and recognising possible money laundering activities. Indeed, there is growing sentiment that combining human insight and processes with AI can drive better outcomes and new ways of working that are more effective than deploying humans or AI in isolation (Craig, 2019). The financial institutions can maintain compliance with regulatory essentials and preserve an intense control atmosphere.

4.3 AI in Customer Service and Experience

With deep expertise in experience strategy and design, data and analytics and platform consulting and implementation harnessing best-in-class solutions, we help you drive transformation across the customer lifecycle, spanning marketing, commerce, sales and service (IBM, n.d.). The utilisation of AI in customer service and experience has modified how financial institutions communicate with customers.

NLP empowers chatbots and virtual assistants to engage in natural and conversational interactions, mimicking human empathy and emotional intelligence (Sadik, 2023). The algorithms offer personalized and efficient customer support, addressing inquiries, providing account information, and assisting with basic banking transactions. The systems improve customer experience by providing 24/7 availability, decreasing response times, and enabling self-service. These systems can manage numerous customer questions, alleviating human help for more complex assignments and enhancing general functional efficiency. Besides, AI-powered analytics permit financial institutions to achieve insights into consumer preferences and behaviour, facilitating personalized product suggestions, targeted marketing campaigns, and tailored financial guidance. However, financial institutions need to balance automation and human interaction to guarantee a seamless client experience. While AI technologies improve efficiency and comfort, the availability of human representatives for more sophisticated inquiries and issue resolution remains essential in maintaining customer satisfaction and trust. The AI technology is relatively new and will continue to evolve and improve (Zendesk, n.d.).

4.4 AI for Operational Productivity Enhancement

AI transforms operational efficiency, quality and competitiveness. Changing customer demands, new business models and disruptive technologies significantly impact operations (Delaware,n.d). Operational productivity enhancement is fundamental for financial institutions aiming to facilitate operations, decrease costs, and enhance prevailing efficiency. AI technologies present considerable possibilities for functional productivity enhancement, from industrialization and procedure optimization to data analysis and decision-making support. Automation and process optimization with AI enable financial institutions to misjudge manual intervention, lower errors, and expedite everyday tasks such as document processing, customer onboarding, and compliance checks. It automates repetitive tasks, streamlines processes, reduces errors, and speeds up decision-making, enabling cost savings and operational efficiency for banks and financial institutions (Finance Digest,2023). The benefit of automating these processes is that financial institutions can reallocate resources, enhance precision, and assign human capital to better value-added activities. The Machine Learning algorithms can investigate market trends, client behaviors, and financial indicators, allowing more knowledgeable investment management, risk assessment, and product maturation decision-making. These AI-powered instruments improve operational efficiency, enable proactive decision-making, and drive innovation within financial institutions. In conclusion, artificial intelligence plays an increasingly important role in our lives and economy and already impacts our world in many ways (Szczepański,2019.)

The European financial and banking sectors are detecting a rapid and expansive adoption of AI technologies. The applications in risk management enhance risk assessment models, optimize capital allowance, and improve risk mitigation procedures. AI-powered fraud detection and prevention systems support detecting and preventing fraudulent actions, defending financial institutions and their clients. AI-driven customer service and knowledge resolutions revolutionize customer interchanges, deliver personalized help, and tailored financial guidance.

Lastly, AI's role in operational productivity enhancement streamlines operations to decrease expenses and delegates financial professionals to make data-driven decisions. As financial institutions continue to embrace AI technologies, the European economic and banking sectors are balanced to leverage the transformative possibility of AI, driving innovation, enhancing customer experiences, and providing tolerable development.

5. Case Study: Deutsche Bank - Implementing AI for Operational Productivity and Cybersecurity

5.1 Overview of Deutsche Bank and its AI Initiatives

Since Deutsche Bank was founded in 1870, its development has been essential to European business history (Deutsche Bank, n.d.). According to the Deutsche Bank quarterly report in June 2023, the bank's revenue consists of 6.66B. Deutsche Bank, a major European financial institution, has been at the vanguard of leveraging Artificial Intelligence technologies to improve operational productivity and boost cybersecurity measures. According to Clarke(2023), Deutsche Bank is looking at how generative AI could help automate people-heavy processes in a potential "game-changer" for the industry, according to one of its top executives -Fabrizio Campelli. With a substantial dedication to innovation, Deutsche Bank has enforced various AI initiatives to streamline procedures, improve decision-making, and mitigate cybersecurity risks. Deutsche Bank recognizes that AI has the potential to revolutionize traditional banking operations by automating routine tasks, improving data analysis, and enhancing overall operational efficiency. The bank has invested substantially in AI research and development, collaborating with leading technology firms and academic institutions to explore cutting-edge AI solutions. The bank is currently investigating three key areas: developing software code that aids developers in boosting productivity, implementing AI chatbots to assist employees and clients with queries using unstructured data and voice, and accelerating risk calculations(Saha,2023).

5.2 AI Applications in Operational Productivity at Deutsche Bank

Automating business processes makes them more efficient. Customers can receive their goods quicker, and payments are made sooner and management(Metcalf-Dennis, n.d.).Automation and process optimization are essential priority areas for the bank, aspiring to reduce manual intervention, improve precision, and expedite everyday tasks. Deutsche Bank is leveraging Machine Learning algorithms that have designed intelligent systems to extract suitable information from documents, verify customer data, and assure adherence to regulatory requirements. These automation actions have saved considerable time and cost, permitting employees to focus on more complex and value-added activities. The official article published by the bank in 2022 stated that" Deutsche Bank and NVIDIA are testing a collection of large language models called Financial Transformers". These will drive AI and ML models and conduct results such as early warning signals on the counterpart of a financial transaction, more rapid data recovery and identifying data-quality issues. Moreover, AI-driven data analysis instruments have been executed to improve decision-making procedures. Deutsche Bank leverages progressive analytics and predictive modelling to explore market directions, client behaviour, and economic indicators.

5.3 Cybersecurity Threats and AI Solutions at Deutsche Bank

Acknowledging the integral significance of cybersecurity in the digital age, Deutsche Bank has leveraged AI technologies to improve its cybersecurity defences.

The bank comprehends that traditional safety measures are no longer acceptable to fight sophisticated cyber threats. Even if Deutsche Bank has introduced AI danger detection techniques to explore vast data and determine abnormal practices that may demonstrate potential cyber-attacks, AI can deliver assertive and intelligent solutions. However, in 2023, the US Federal Reserve issued a \$186 million fine to Deutsche Bank over anti-money laundering (AML) failures yearly this year. The central bank said the penalty concerns "unsafe and unsound" practices and violations of the board's 2015 and 2017 consent orders linked to sanctions compliance and AML controls(Leonards,2023).The benefit of Machine Learning algorithms constantly learns from new data, adapting to developing threats and decreasing false positives will help the organization. These systems enable early detection and response to potential security breaches, protecting sensitive customer information and the bank's infrastructure.Besides, AI irregularity detection tools have been enforced to identify unauthorized entry attempts and detect irregular bank system behaviour. These instruments can rapidly recognise security violations and mitigate threats by observing network traffic, user behaviour, and procedure logs.

5.4 Challenges and Successes in AI Implementation: Lessons from Deutsche Bank

Enforcing AI initiatives at Deutsche Bank has come with its challenges and successes. It continues to unlock new growth opportunities and competitive advantages for a diverse range of organizations and their stakeholders – and is being used for everything from a better understanding of diseases to creating a fairer, more robust financial market(Corporates.db.com,n.d).One of the primary challenges the bank fronts is the need for vigorous data management and quality. AI algorithms laboriously rely on valid and reliable data, and Deutsche Bank has focused on guaranteeing data integrity and availability. The bank has funded data management frameworks and enforced data governance methods to manage these challenges. Deutsche Bank contributed to a **\$14.2m round** for Finanzguru, the developer of an AI-powered banking assistant, in April this year(Lavine, 2023). Finanzguru represents democratizing access to financial well-being by removing complexity from personal financial management (PayPal Newsroom, 2023). A further challenge lies in the ethical and accountable use of AI.

Deutsche Bank acknowledges the significance of using AI technologies to keep customer confidence and privacy. The bank has enforced stringent ethical policies and privacy standards to assure compliance with regulatory conditions and guard consumer data.

Despite these challenges, Deutsche Bank has reached considerable success in AI implementation. The bank has undergone improved operating efficiency, decreased expenses, and improved decision-making procedures. The AI ambitions have helped Deutsche Bank to automate time-consuming jobs, optimize resource distribution, and support cybersecurity standards. Deutsche Bank's successes spotlight AI's transformative possibility in the financial sector. The lessons learned from their implementation journey provide valuable insights for other financial institutions seeking to embark on similar AI initiatives. According to the Australian Financial Review article (2023), Deutsche Bank is deploying so-called deep learning to analyse whether international private banking clients are too heavily invested in a particular asset and match individual customers with suitable funds, bonds or shares. Institutions must design an explicit strategy, establish robust data management practices, secure the ethical usage of AI, and promote a culture of innovation and collaboration.

In closing, Deutsche Bank's performance of AI for operating productivity and cybersecurity indicates its commitment to leveraging advanced technologies to improve business approaches and protect against cyber threats. The bank's automation, data analysis, and danger detection industries demonstrate AI's possibility to change traditional banking procedures. By adopting AI, Deutsche Bank has become a leader in embracing AI technologies within the European financial sector, appointing a benchmark for different organisations.

5.5 Case Study: HSBC Bank - Ayasdi: AI for Anti-Money Laundering

5.6 Overview of HSBC Bank and its AI Initiatives

HSBC Holdings plc (in full: Hong Kong and Shanghai Banking Corporation) is a British universal bank and financial services group headquartered in London, England, with unique historical and business links to East Asia and a highly multinational footprint. Hong Kong and Shanghai Banking Corporation, known as HSBC Holdings plc is a universal British bank serving around 39 million personal, wealthy and corporate customers worldwide in 62 countries and territories(HSBC website,n.). HSBC Bank, one of the largest global banking institutions with more than 150 years of activity, has now recognized the potential of Artificial Intelligence in combating financial crimes, particularly in anti-money laundering. To support its AML measures, HSBC has cooperated with Silicon Valley-based artificial intelligence startup Ayasdi (SymphonyAI Sensa-NetReveal, n.d.), an AI technology provider specializing in progressive analytics and machine learning.

5.7 Ayasdi's AI Solution for Anti-Money Laundering

Ayasdi's AI solution delivers HSBC Bank a complete approach to catching and stopping money laundering actions. The resolution utilizes refined analytics, machine learning, and network investigation methods to recognize complex procedures and irregularities of suspect transactions. By investigating considerable volumes of transactional data, Ayasdi's AI resolution can determine hidden relationships, notice uncommon behaviour, and find possible money laundering actions that may have gone overlooked, utilising traditional rule-based approaches. By investigating considerable volumes of transactional data, Ayasdi's AI resolution can determine hidden relationships, notice uncommon behaviour, and find possible money laundering actions that may have gone overlooked, utilising traditional rule-based approaches. This AI-powered system allows HSBC Bank to improve its capacity to recognise and mitigate money laundering threats. Ayasdi's AI resolution also suggests real-time monitoring abilities, permitting HSBC Bank to investigate transactions and determine possible risks as they appear constantly. The resolution can deliver signals and develop actionable insights, facilitating the bank's AML team to react effectively to potential threats. Using the AyasdiAI dramatically reduces the time to achieve genuine transparency with full explainability (SymphonyAI Sensa-NetReveal, 2021).

5.8 Benefits and Successes of Ayasdi's AI Solution at HSBC Bank

Introducing Ayasdi's AI solution at HSBC Bank has generated several advantages and triumphs in the combat against money laundering. Firstly, the solution has enhanced detection precision by decreasing false positives and letting the bank's AML team concentrate on actual threats. Using this new solution, HSBC has purportedly reduced false positive investigations by 20%(Mixon, 2021). By employing evolved analytics and machine learning algorithms, Ayasdi's AI solution can recognise complicated and delicate practices of money laundering that may enclose evaded traditional rule-based systems. Secondly, Ayasdi's AI solution has improved operating efficiency by automating time-consuming manual operations. The resolution can manage considerable volumes of data and develop actionable insights in real-time, allowing the bank's AML team to make faster and more instructed decisions. This automation has sweetened efficiency and sheds up help, permitting AML investigators to focus on more complicated, high-risk cases. Likewise, Ayasdi's AI solution has supplied HSBC Bank with a more aggressive and forward-looking strategy for fighting money laundering. The chair of the Technology Advisory Board at HSBC Global COO, Andy Maguire, said: "We have made significant progress in the last couple of years, including becoming the most influential financial services user of biometrics globally through Touch ID, Voice ID and facial recognition, and our participation in the first use of blockchain in trade finance (Ayasdi,2017). " The resolution's capability to catch emerging practices and adapt to evolving money laundering procedures encourages the bank to bypass potential risks. This proactive process is crucial in fighting financial crime's dynamic and ever-changing nature.

5.9 Challenges and Lessons Learned from AI Implementation at HSBC Bank

While enforcing Ayasdi's AI solution has produced considerable advantages, HSBC Bank has also faced challenges. One substantial challenge is incorporating the AI solution with the bank's existing infrastructure and systems. Providing seamless data discharge and compatibility between Ayasdi's AI solution and HSBC Bank's internal systems demands detailed planning and cooperation between the players. Another challenge lies in the understanding and explainability of the AI explanation's results. As AI algorithms examine extensive quantities of data and recognise complicated patterns, it evolves essential for AML investigators to comprehend and define the cause behind the AI-generated warnings. The bank could then understand these models because they were made using terms they were already familiar wit. (Mejia, 2020).HSBC Bank has managed this challenge by training its AML team extensively on the AI solution's functionality and outcomes.

Executing Ayasdi's AI solution at HSBC Bank has furnished practical studies for other financial organisations aiming to improve their AML measures employing AI. Institutions must finance powerful data management systems, ensure proper integration with existing infrastructure, and deliver extensive activity to staff to use AI solutions for AML.

In conclusion, HSBC Bank's partnership with Ayasdi and the performance of their AI solution for anti-money laundering have yielded considerable progress in catching and preventing financial offences. By leveraging developed analytics and machine learning, HSBC Bank has improved its capability to recognise dubious transactions, lower false positives, and automate manual procedures. As compliance costs continue to rise, HSBC has partnered with AI startup Ayasdi to fight money laundering more efficiently (Back, 2017). This case study emphasises the possibility of AI in supporting AML measures and presents HSBC Bank's dedication to utilizing creative technologies to combat financial crimes effectively.

6. Cybersecurity Threats and Data Privacy Challenges in the European Financial and Banking Sector

6.1 Overview of Cybersecurity Threats in the Financial and Banking Sectors

The financial sector has always been considered to have a wide array of secure and protected systems due to its continuous dealing with private information and handling of large sums of money (Sangfor Technologies, 2022).

However, the European financial and banking sector meets considerable cybersecurity threats, which have evolved increasingly sophisticated and pose substantial dangers to institutions and their clients. These include various forms of cyber attacks, data breaches, and unauthorized admission to sensitive data. One standard cybersecurity threat is phishing, where attackers trick individuals into revealing confidential information through fraudulent emails or websites, such as login credentials or financial details. Phishing is among the most common and dangerous Internet crimes transactions (HSBC, 2021). Phishing attacks can direct to unauthorized entrance to client accounts, identity theft, and financial losses. Malware is another significant threat, malicious software developed to disrupt computer systems, swipe data, or earn unauthorized access. Malware can be submitted through contaminated attachments, downloads, or compromised websites, posing a considerable risk to the safety of financial and banking systems. The relationship between Artificial Intelligence and malware intersects in numerous proportions. AI and malware are broad fields, and their convergence has led to the evolution of the cybersecurity landscape in diverse ways. Besides, Distributed Denial of Service (DDoS) attacks can overwhelm a bank's network infrastructure, rendering its services unavailable to customers.

The most obvious symptom of a DDoS attack is a site or service suddenly becoming slow or unavailable(Cloudflare,2022).

These attacks involve flooding the network with overwhelming traffic, causing disruptions, financial losses, and damage to the bank's reputation.

7. Mitigating Cybersecurity Threats: Best Practices and Solutions

A robust cybersecurity risk management plan is critical to help your organization reduce exposure to cyber threats.(www.jpmorgan.com, n.d.).To mitigate cybersecurity threats and manage data privacy challenges, European financial and banking organizations must implement powerful cybersecurity measures and adopt the most promising procedures. Some fundamental techniques and solutions contain:

- Implementing multi-factor authentication to strengthen access controls and protect against unauthorized access.
- Regularly updating and patching software systems to address known vulnerabilities and protect against malware and cyber-attacks.
- Employing advanced encryption techniques to secure and protect sensitive data from unauthorized access.
- Conduct regular cybersecurity awareness training for employees to educate them about potential threats, phishing attacks, and safe online practices.
- Employing AI-driven threat intelligence systems to detect and respond to cyber threats in real time, enhancing incident response capabilities.
- Collaborating with industry peers and sharing threat intelligence to stay updated on emerging cyber threats and best practices.
- Conduct regular penetration testing and vulnerability assessments to identify and address weaknesses in the system.
- Ensuring compliance with data protection regulations, such as GDPR, and adopting privacy-by-design principles when implementing AI-driven systems.

In closing, the European financial and banking sector meets critical cybersecurity threats and data privacy challenges. Phishing, malware, and DDoS attacks are expected threats targeting financial organisations. With AI-driven methods, data privacy situations arise, necessitating detailed managing and safeguarding of customer details. Exposures and risks associated with AI adoption, such as intolerance and malicious attacks, direct awareness and mitigation.

Enforcing best practices and robust cybersecurity standards, including multi-factor authentication, encryption, and threat intelligence systems, can help mitigate these threats and protect the integrity and safety of Europe's financial and banking sectors.

8.The Cyber Threat of AI in the Banking System: Considerations from the Customer's Perspective

8.1 Introduction to AI-related Cyber Threats in the Banking System

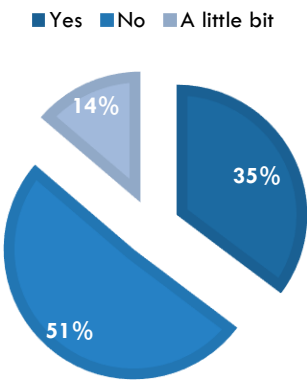
The beginning of artificial intelligence has experienced a new boom, mainly due to the considerable improvement in the computing power of computers and access to massive quantities of data.(Council of Europe, 2014). This advancement carried influential progress and convenience to diverse sectors, including the banking system. This technological progress has also presented new challenges and openness, especially concerning cyber threats.

AI-related cyber threats pose a considerable crisis in the banking industry, as they can compromise the safety and privacy of client data, financial transactions, and prevailing confidence in the system.

The author will interpret the result collected in the questionnaire (Appendix No?) to manage valuable understandings concerning the knowledge, awareness, and perceptions of AI-related cyber threats in the banking system from customers (students at the University of Wales Trinity Saint David) perspectives.

Analyzing the questionnaire results based on 51 responder on understanding AI-related cyber threats indicates that a significant 51% of the students need to become more knowledgeable about these threats 35% of responder here familiar with the Cyber Threats and 14% were just a little bit aware.

DIAGRAM NO 1.ARE YOU FAMILIAR WITH THE AI-RELATED CYBER THREATS?



Given the supplied data, we can calculate the mean that represents a measure of the central tendency of a probability distribution along median and mode (Taylor, 2022). The mean is calculated by adding up all the percentages and then dividing by the number of categories (in this case, 3):

$$Mean = \frac{51 + 35 + 14}{3} = \frac{100}{3} = 33,3\%$$

Equation No 1.The mean Eads,A.(2023).

Nevertheless, employing the percentages supplied to calculate the mean might need to be more accurate, as we consider percentages of different varieties instead of raw data particulars. The middle number in a sorted ascending or descending list of numbers represents the median (Taylor, 2022) and can be more descriptive of that data set than the average. In the three categories and rationed percentages, the median is 35% since it's the middle value between 14%, 35%, and 51%.

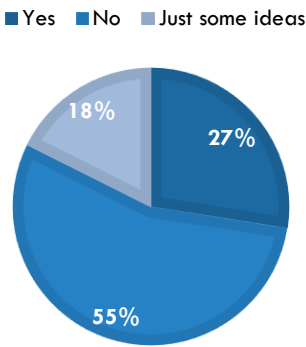
The mode is the value that appears the most often in a data set, and it can be used as a measure of central tendency, like the median and mean (Government of Canada, S.C. and Government of Canada, S.C,2002) Occasionally, there is no mode, as is this example, since each percentage compares to a distinctive type, and none are repeated.

This finding underlines the demand for more awareness among the student concerning the possible dangers associated with AI technology in the context of cyber threats.

8.2 Phishing Attacks: Exploiting AI for Social Engineering

Analyzing the questionnaire results about students' awareness of phishing attacks leveraging AI for social engineering purposes reveal that a considerable prevalence, 55%, has yet to learn about these distinct attacks.

DIAGRAM NO 2. HAVE YOU HEARD ABOUT PHISHING ATTACKS LEVERAGING AI FOR SOCIAL ENGINEERING PURPOSES?



This result highlights a demand for more understanding among the students about the convergence of AI and social engineering methods in the context of phishing attacks. Nevertheless, it is worth mentioning that 27% of the students replied affirmatively, suggesting they are conscious of phishing attacks. This subset of respondents indicates a more elevated level of understanding and knowledge in identifying the possible risks of integrating AI and phishing techniques. Likewise, 18% of the students reported having some ideas about these attacks, indicating a partial understanding of the topic. These results highlight the need for increased education and awareness campaigns explicitly targeting the intersection of AI and social engineering in the context of phishing attacks.

The survey results demonstrate that multiple students need more understanding of phishing attacks leveraging AI for social engineering goals. Nevertheless, some respondents suggested knowledge or partial implementation of these threats. To manage this hole, it is essential to prioritize academic standards and provide students with the ability and skills to identify and mitigate the dangers associated with AI-powered phishing attacks.

Nevertheless, employing the percentages supplied to calculate the mean might need to be more accurate, as we consider percentages of different varieties instead of raw data particulars. The middle number in a sorted ascending or descending list of numbers represents the median (Taylor, 2022) and can be more descriptive of that data set than the average. In the three categories and rationed percentages, the median is 35% since it's the middle value between 14%, 35%, and 51%.

The mode is the value that appears the most often in a data set, and it can be used as a measure of central tendency, like the median and mean (Government of Canada, S.C. and Government of Canada, S.C.,2002) Occasionally, there is no mode, as is this example, since each percentage compares to a distinctive type, and none are repeated.

This finding underlines the demand for more awareness among the student concerning the possible dangers associated with AI technology in the context of cyber threats.

8.3 Deepfake Fraud: Impersonation and Manipulation with AI-generated Content

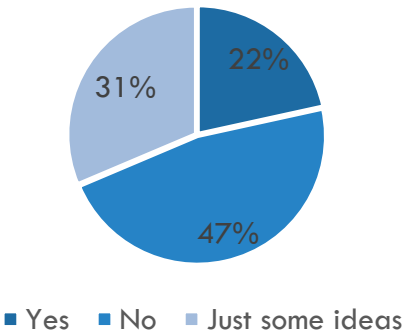
Since the first Terminator movie was released, we have seen portrayals of robots taking over the world. Now we are at the beginning of a process by which technology—specifically, artificial intelligence (AI)—will enable the disruption of the entertainment and media industries themselves (Vejay et al., 2022). According to the Cambridge Dictionary (n.d), deepfake means: "a video or sound recording that replaces someone's face or voice with that of someone else, in a way that appears real". Deepfake technology, powered by AI, poses a considerable danger to the banking system. This process involves producing highly realistic artificial media for malicious intentions, including audio and videotape. In 2020, threat actors used an audio-deep fake to steal \$35 million from a Hong Kong bank, the most significant publicly disclosed amount lost to inauthentic content yet (Brewster, 2021).

Cybercriminals use deep fakes to impersonate clients, bank workers, or other trustworthy entities, conducting fraudulent activities such as unauthorized admission to accounts or manipulating financial transactions.

The cosmopolitan essence of deepfakes causes it difficult for clients to distinguish between real and fraudulent interactions. While deepfake technology is still fairly new (first developed in 2017), deep fakes rank as one of the most dangerous AI crimes of the future(Bank of America,n.d). The questionnaire's results on comprehending deep fake fraud, which involves impersonation and manipulation utilizing AI-generated range, show that 47% of the students surveyed are unaware of this precise variety of fraud. This finding indicates a substantial need for more acquaintance among the students about the risks and importance of deepfake in the context of fraudulent actions. Interestingly, about 31% of a substantial portion appeared to have a partial familiarity or had only heard about this subject. On the other hand, 22%% of the students answered affirmatively, suggesting they are familiar with deep fake fraud and its possible effect. This subset of respondents demonstrates a higher level of knowledge and understanding regarding using AI-generated content for impersonation and manipulation. The results highlight the significance of increasing awareness about deepfake fraud, especially among students' potential to be active digital media and social platform customers.

Deepfake technology can potentially mislead individuals by making highly realistic synthetic media, including audio and video, which can be exploited for fraudulent activities such as impersonation or manipulation of information. Educational institutions should consider incorporating specific modules or workshops on deep fake fraud within their cybersecurity curricula or media literacy programs. These initiatives can help students understand the techniques used to create deep fakes, raise awareness about the potential risks associated with their proliferation, and provide guidance on identifying and mitigating the impact of deep fake fraud. Furthermore, collaborations between educational institutions, cybersecurity experts, and technology industry stakeholders can contribute to ongoing research and development in detecting and combating deep fake fraud. Investing in advanced detection technologies and promoting responsible use of AI-generated content makes it possible to undervalue the potential damage induced by deep fake fraud and protect individuals from such deceptive practices.

DIAGRAM NO 3. ARE YOU AWARE OF DEEPPFAKE FRAUD,WHICH INVOLVES IMPERSONATION AND MANIPULATION USING AI GENERATED CONTENT

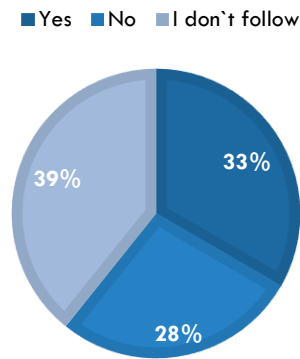


The survey derivatives demonstrate that numerous students do not understand deep fake fraud, which affects impersonation and manipulation using AI-powered content. Measures should be taken to enhance instruction and awareness regarding this hazard, supplying students with the ability and skills to recognise and react properly to deep, fake-based fraudulent actions. By promoting media literacy and cybersecurity awareness, people can become better resilient to the probable risks connected with deepfake technology.

8.4 Being Wary of Suspicious Communications

As technology advances at an unprecedented rate, artificial intelligence has become increasingly prevalent in many areas of our lives(Van Rijmenam, 2023). Customers must exercise vigilance when accepting emails, messages, or phone calls requesting confidential or financial information. Confirming the genuineness of such contacts via trusted channels, such as contacting the bank directly, can help mitigate the risk of falling victim to phishing attacks or deepfake fraud. Recently the conveyancing industry has become a victim of this online crime.

DIAGRAM NO 4.ARE YOU AWARE OF
PRIVACY CONCERNS RELATED TO AI, SUCH
AS DATA BREACHES AND UNAUTHORIZED
ACCESS?



Homebuyers/sellers and solicitors have lost more than £10m in the last year(Barclays.co.uk,n.d.). The survey outcomes exhibit that 33% of the respondents are conscious of privacy concerns connected to AI, such as data violations and unauthorized access. This subset of participants illustrates a comprehension of the possible risks and importance of AI concerning privacy. They admit that AI systems can be powerless against data breaches and unauthorized access, which can reveal sensitive data and compromise privacy. Unaware of these privacy concerns related to AI, 28% of respondents. This result emphasizes a significant understanding gap among the studied population about the privacy importance of using AI.

These people may be required to comprehensively understand the dangers and consequences of data breaches or unauthorized access. It is worth mentioning that 39% of the respondents notified had a fundamental understanding of privacy concerns related to AI, but they do not follow this topic. While they may need comprehensive familiarity, they have at least listened to or discovered some details about the topic. The outcomes highlight the significance of boosting the general population's cognition about privacy concerns associated with AI.

8.5 Banks' Efforts in Ensuring Security and Privacy

Banks are responsible for implementing robust security measures to safeguard customer data and mitigate AI-related cyber threats. According to HSBC(n,d), the bank will continue to check with fraud prevention agencies to prevent fraud and money laundering and confirm your identity before we provide products and services to customers. This action incorporates funding for developed threat detection systems that leverage AI algorithms to effectively recognize and react to growing cyber threats. Banks must also prioritize consumer education by delivering explicit guidelines, safety awareness campaigns, and continued help to assist clients in navigating the ever-changing landscape of AI-powered cyber threats. In conclusion, the increasing integration of AI technology into the banking system brings benefits and risks. According to Natwest Bank (n,d), for all financial institutions, AI is both a tool for managing risk and a source of significant new risks that must be managed. While AI supplies efficiency and enhanced client experiences, it exposes customers to cyber threats. Among customers ' significant threats are phishing attacks, deep fake fraud, synthetic identity theft, malware and botnets, and privacy concerns.

Consumers can vigorously mitigate the risks by embracing preventive steps, remaining educated, and working collaboratively with banks. Simultaneously, banks must continue to fund security efforts, educate clients, and prioritize protecting customer data to guarantee a safe and reliable banking domain. As the questionnaire answers demonstrated, most students are not prepared and safe online. Educational institutions and banks must collaborate to create programs of awareness.

9. Regulatory Frameworks and Ethical Considerations in AI Implementation

Regulatory frameworks and moral concerns are essential in implementing Artificial Intelligence in the financial and banking sector. According to UNESCO(2022), in no other field is the ethical compass more relevant than in artificial intelligence. The frameworks designed aim to guarantee the trustworthy and ethical usage of AI while managing possible risks and protecting the rights of people and institutions. This section analyses the regulatory landscape and ethical considerations covering AI performance in the European financial and banking sector.

9.1 Overview of AI-related Regulations in the European Financial and Banking Sectors

The European Union has carried aggressive measures to set regulatory frameworks for AI undertaking, identifying the demand for AI's transparent, responsible, and suitable benefit. The General Data Protection Regulation (GDPR) imposes severe data safeguard measures, demanding financial organizations receive unambiguous permission for data processing, secure data security, and deliver individuals with ownership over their data. According to the GDPR act, organisations and individuals must inform the customer what information they hold about them and how it is being used. This means that if companies use artificial intelligence to process someone's data, they must tell them about it (Church,n.d). GDPR also sets limitations on automatic decision-making, including profiling, to safeguard individuals' rights and prevent intolerance. In complement to GDPR, the EU has suggested the AI Act, a complete regulatory framework managing AI systems. The AI Act offsets innovation by defending essential rights and ethical concerns. In April 2021, the European Commission proposed the AI Act, a draft legislation setting out rules for governing AI within the EU. The AI Act would establish four levels of risk for AI: unacceptable risk, high risk, limited risk, and minimal risk(Tobin,2023). It classifies AI systems into risk classifications and assesses duties, including transparency, human oversight, and risk management. It also specifies a European Artificial Intelligence Board to oversee the performance and enforcement of the AI Act. Furthermore, regulatory authorities such as the European Banking Authority (EBA) and the European Securities and Markets Authority (ESMA) have issued guidelines and recommendations for using AI in the financial sector. The European Banking Authority (EBA) published a follow-up report on the 4th of August 2023, presenting the feedback received during the consultation on machine learning. According to the input, using ML techniques in credit risk models may create issues beyond the scope of prudential consideration.

In this respect, this follow-up Report also discussed the interaction with two other legal frameworks, namely the General Data Protection Regulation and the Artificial Intelligence Act and called for some clarifications to reduce legal uncertainty and avoid unintended consequences of the AI Act European Banking Authority. (2023). These approaches highlight the necessity for trustworthy AI governance, risk control frameworks, and the explainability of AI standards to guarantee transparency and responsibility.

The UK government publicised. 'A pro-innovation approach to AI regulation' is named White Paper, which provides a framework for the UK's procedure for regulating AI.

The government has chosen to refrain from legislating to build a single process to supervise the principles of AI. According to Heywood(2023), to support existing regulators, develop a sector-focused, principles-based approach. Regulators, including the ICO, the CMA, the FCA, Ofcom, the Health and Safety Executive, the MHRA and the Human Rights Commission, will be required to consider the following five principles to build trust and provide clarity for innovation: safety, security and robustness transparency and explain ability fairness accountability and governance contestability and redress.

In conclusion, regulatory frameworks and ethical considerations are integral to AI's successful and responsible implementation in the European financial and banking sector. With AI technologies extending staggeringly, the time is now to implement best practices to promote AI (Clancy et al.,2023). The EU has designated laws such as GDPR and proposed the AI Act to safeguard individuals' rights and ethical use of AI. Financial organisations must adopt ethical considerations in their AI performances, including transparency, fairness, responsibility, and data privacy. By embracing complete governance frameworks, showing honourable impact assessments, and incorporating trustworthy AI practices, financial institutions can guide the regulatory landscape and manage moral challenges while harnessing the benefits of AI responsibly and ethically.

10. Prospects of AI in the European Financial and Banking Area

10.1 Emerging Trends and Technologies in AI

The opportunities for Artificial Intelligence in the European monetary and banking sector are up-and-coming, with rising tendencies and technologies balanced to revolutionise the industry. You call artificial intelligence and machine learning magic. On the contrary, your friend deems it as just another revolution – devouring some jobs, flooding with a double of new jobs.

While this debate continues in the chorus, PwC's global AI study says that the global economy will see a boost of 14% in GDP by 2030, amounting to a potential increase of \$15.7 trillion (Avcontentteam, 2023). AI can enhance operating efficiency, improve client experience, and allow more precise decision-making. This section examines the fundamental opportunities and trends in AI that are expected to shape the future of banks. In the next five to 10 years, there are several key trends expected to shape the financial services industry (Hussain, 2023). One major trend is the increasing use of machine learning algorithms for predictive analytics and risk management. Different algorithms can be used in machine learning for other tasks, such as simple linear regression that can be used for prediction problems like stock market prediction, and the KNN algorithm can be used for classification problems (www.javatpoint.com, n.d.). They can analyse extensive data and recognise practices and trends to support financial institutions in making more informed decisions. By leveraging historical data, machine learning algorithms can enhance credit scoring standards, notice fraudulent actions, and optimise risk management strategies.

Furthermore, the emergence of robotic process automation (RPA) and intelligent process automation (IPA) technologies offers opportunities for streamlining operations and reducing manual efforts. RPA enables the automation of repetitive tasks, such as data entry and document processing, and uses software bots to automate repetitive tasks, freeing up human time for more complex work and thereby boosting business efficiency (www.automationanywhere.com, n.d.). IPA combines RPA with AI capabilities and is the product of the convergence of AI and related technologies – including computer vision, cognitive automation and machine learning – with RPA (NICE Systems, n.d.). AI-based systems are now helping banks reduce costs by increasing productivity and making decisions based on information unfathomable to a human. Also, intelligent algorithms can spot fraudulent information in seconds (appinventiv. com, 2023). By designing a clear AI strategy, fostering a data-driven culture, investing in talent and skills, collaborating with partners, and ensuring ethical practices, financial institutions can leverage the potential of AI to transform their operations and better serve their customers in the evolving economic landscape. Please see the Findings table number 1.

11. Conclusion

In conclusion, the possibilities of AI in the European financial and banking sector are significant, delivering prospects for enhanced operating efficiency, enhanced client experience, refined risk management, and data-driven decision-making.

The first hypothesis was proven with the rise of sophisticated AI-driven cyber threats such as deepfakes and progressive phishing strategies; this hypothesis aspires to demonstrate a correlation between AI adaptation and exposure that the companies may experience.

The second hypothesis was partially proven; recognizing the evolving nature of cyber threats, this hypothesis postulates that AI-driven behavior authentication, which can quickly adapt to new threat patterns, offers superior security.

The questionnaire revealed the necessity of educating customers regarding the cyber threat and that the banks need to train customers to be more aware of online dangers.

The third hypothesis is proven by promoting worldly AI-driven cyber threats such as deepfakes and advanced phishing schemes; this hypothesis aims to showed a correlation between AI adoption and vulnerability.

Financial institutions that adopt AI technologies and guide the associated challenges can achieve a competitive advantage in the market. AI's transformative impact has been profound since its advent, changing how enterprises, including those in the banking and finance sector, operate and deliver customer services.

The introduction of AI in banking apps and services has made the industry more customer-centric and technologically relevant.

11.1 Recommendations for Successful AI Integration

Successfully integrating AI technologies required a holistic transformation spanning multiple layers of the organization (Biswas et al., 2020). Financial institutions should consider the following recommendations:

- a) **Develop a Clear AI Strategy:** Financial institutions should develop a comprehensive AI strategy that aligns with their business objectives, regulatory requirements, and risk appetite. This strategy should outline the areas where AI can bring the most value and define a roadmap for implementation.
- b) **Foster a Data-Driven Culture:** Financial institutions should establish a data-driven culture emphasising the importance of data quality, governance, and privacy. This involves investing in data infrastructure, ensuring data security, and promoting employee data literacy.
- c) **Invest in Talent and Skills:** Financial institutions should build a diverse team of AI experts, data scientists, and domain specialists who can drive AI initiatives. This includes providing training and upskilling opportunities to employees to enhance their understanding of AI technologies and their application in the financial domain.
- d) **Collaborate and Partner:** Financial institutions should explore collaborations with technology providers, academic institutions, and industry peers to leverage expertise, share best practices, and drive innovation in AI. Partnerships can help accelerate AI adoption, mitigate implementation challenges, and foster knowledge sharing.
- e) **Ensure Ethical and Responsible AI Practices:** Financial institutions must prioritise ethical considerations and responsible AI practices. This includes addressing algorithm bias, ensuring transparency and explainability in AI models, and protecting customer privacy and data security. Compliance with regulatory frameworks like GDPR is essential to maintain trust and mitigate reputational risks.

12. Summary of Findings

Finding	Summary
Familiarity with AI-related cyber threats	The questionnaire outcomes suggest a demand for more understanding among the student population regarding AI-related cyber threats in the banking system. Most students reported unfamiliarity with these threats, suggesting a significant knowledge gap in understanding the potential risks associated with AI technology.
Awareness of phishing attacks leveraging AI	The findings show that many students are unaware of phishing attacks that exploit AI for social engineering purposes. This highlights a need for more understanding among students regarding the specific threat of AI-powered phishing attacks, which can be highly deceptive and lead to financial losses or data breaches.
Awareness of deep fake fraud	Approximately one-third of the students indicated that they know deep fake scams involving impersonation and manipulation using AI-generated content. This subset of respondents demonstrates a moderate level of knowledge regarding the potential risks and implications of deepfake technology, highlighting an understanding of the deceptive nature of AI-generated synthetic media.
Personal information protection measures	The survey results reveal that many students prioritize protecting their personal information. The respondents reported using strong passwords to safeguard their data. This indicates a positive cybersecurity practice, as strong and unique passwords can help prevent unauthorized access to online accounts
Awareness of privacy concerns related to AI	:The findings show that most students are unaware of privacy concerns associated with AI, such as data breaches and unauthorized access. This underscores a knowledge gap in understanding AI technology's potential privacy risks, indicating a need for greater awareness and education in this area.

12.1 Contributions to Knowledge

This study on the awareness of AI-related cyber threats, phishing attacks leveraging AI, deep fake fraud, personal information protection, and privacy concerns related to AI in the banking system contributes to the existing body of knowledge in several ways.

Firstly, the findings highlight the extent of the knowledge gap among students regarding AI-related cyber threats in the banking system. The results indicate a significant need for more familiarity with these threats, emphasizing educational initiatives and awareness campaigns to bridge this gap. This contributes to understanding the current level of awareness among the student population, which can inform the development of targeted educational programs to enhance cybersecurity knowledge.

Secondly, the study sheds light on the specific areas where students need more awareness. The findings reveal a lack of understanding regarding phishing attacks that leverage AI for social engineering purposes and privacy concerns related to AI. This contributes to identifying key knowledge gaps and provides valuable insights for policymakers, educators, and cybersecurity professionals to develop strategies to address these specific areas of concern.

Moreover, the study uncovers students' varying levels of awareness regarding deep fake fraud. The findings indicate a moderate level of knowledge among a subset of respondents, highlighting the importance of raising awareness about the deceptive nature of deepfake technology. This contributes to understanding the level of awareness among students and emphasizes the need for educational efforts to inform individuals about the risks and implications of deepfake fraud.

The study also reveals that many students prioritize protecting personal information by using strong passwords. This finding contributes to understanding students' cybersecurity practices and underscores the importance of promoting secure password practices as a fundamental aspect of personal data protection.

Lastly, the study contributes to the overall knowledge base by highlighting the specific areas that require attention and improvement in educating students about AI-related cyber threats and privacy concerns in the banking system. The findings serve as a basis for further research and developing educational materials, awareness campaigns, and policy recommendations to enhance cybersecurity knowledge and promote responsible use of AI technology.

Overall, this study makes a valuable contribution to the existing knowledge by identifying knowledge gaps, highlighting specific areas of concern, and emphasizing the need for educational efforts to enhance awareness and understanding of AI-related cyber threats and privacy concerns in the banking system.

13.Reference list

Appinventiv.com. (2023). *AI in Banking – How Artificial Intelligence is Used in Banks*.

[online] Available at: <https://appinventiv.com/blog/ai-in-banking/amp/>.

Ayasdi (2017). *Ayasdi CEO Gurjeet Singh Named to HSBC Technology Advisory Board*.

[online] www.prnewswire.com. Available at: <https://www.prnewswire.com/news-releases/ayasdi-ceo-gurjeet-singh-named-to-hsbc-technology-advisory-board-300391573>.

Sadik,R.R.(2023). *The Importance of Natural Language Processing in Chatbots and*

Virtual Assistants: Unleashing the Power of Human-Like Interactions. [online] Available

at: <https://www.linkedin.com/pulse/importance-natural-language-processing-chatbots-power-rachman-sedik/> [Accessed 15 Aug. 2023].

Analytics Software & Solutions(2019). *What is Natural Language Processing?* [online]

Available at: https://www.sas.com/en_gb/insights/analytics/what-is-natural-language-processing-nlp.html.

Atkins,S.(2021).AI for banks: Key ethical and security risks.Available at:AI for banks:

Key ethical and security risks | Global law firm | Norton Rose Fulbright.

Australian Financial Review. (2023). *Wall Street banks seizing AI to rewire world of*

finance. [online] Available at: <https://www.afr.com/technology/wall-street-banks-seizing-ai-to-rewire-world-of-finance-20230601-p5dd3o>.

Avcontent Team (2023). *Emerging Trends in AI and ML in 2023 & Beyond*. [online]

Analytics Vidhya. Available at: <https://www.analyticsvidhya.com/blog/2023/05/emerging-trends-in-ai-and-machine-learning/>.

Back, A. (2017). *HSBC to combat money laundering with artificial intelligence*. [online]

Available at: <https://disruptive.asia/hsbc-money-laundering-ai/> [Accessed 16 Aug. 2023].

Banco de España. (n.d.). *The ESCB, the Eurosystem, the ECB and the national central*

banks. [online] Available at: <https://www.bde.es/wbe/en/sobre-banco/actividad-europea/eurosistema-sebc/organizacion-eurosistema/sebc-eurosistema-bce-bancos-centrales/#:~:text=The%20European%20System%20of%20Central> [Accessed 11 Jul.

2023]. Bank of America. (n.d.). *Deepfakes: What They Are & How Your Business Is at*

Risk. [online] Available at: <https://business.bofa.com/en-us/content/cyber-security-journal/deepfakes-business-risks.html> [Accessed 22 Aug. 2023].

Bank, E.C. (2023). Financial Stability Review, May 2023. www.ecb.europa.eu.

[online]Available at: <https://www.ecb.europa.eu/pub/financial>

[stability/fsr/html/ecb.fsr202305~65f8cb74d7.en.html](https://www.ecb.europa.eu/pub/financial).

Biswas, S., Carson, B., Chung, V., Singh, S. and Thomas, R. (2020). *AI in banking: Can banks meet the challenge?* [online] McKinsey. Available at: <https://www.mckinsey.com/industries/financial-services/our-insights/ai-bank-of-the-future-can-banks-meet-the-ai-challenge>.

Booth,A. (2023). *Explaining explainable AI*. [online] Available at: <https://www.gbm.hsbc.com/en-gb/feed/innovation/explaining-explainable-ai#:~:text=Explainable%20AI%20is%20just%20one> [Accessed 14 Aug. 2023].

Boukherouaa, E.B., AlAjmi, K., Deodoro, J., Farias, A. and Ravikumar, R. (2021). Powering the Digital Economy: Opportunities and Risks of Artificial Intelligence in Finance. *Departmental Papers*, [online] 2021(024). doi:<https://doi.org/10.5089/9781589063952.087.A001>.

Brewster,T.(2021) . “Fraudsters Cloned Company Director’s Voice in \$35 Million Bank Heist, Police Find,”. *Forbes*.

Cheatham, B., Javanmardian, K. and Samandari, H. (2019). *Confronting AI risks* | McKinsey. [online] [www.mckinsey.com](https://www.mckinsey.com/capabilities/quantumblack/our-insights/confronting-the-risks-of-artificial-intelligence). Available at: <https://www.mckinsey.com/capabilities/quantumblack/our-insights/confronting-the-risks-of-artificial-intelligence>.

Church, P.(n.d.). *AI & the GDPR: Regulating the minds of machines* | DigiLinks | Linklaters. [online] Available at: <https://www.linklaters.com/en/insights/blogs/digilinks/ai-and-the-gdpr-regulating-the-minds-of-machines#:~:text=Transparency%20and%20%E2%80%9Cexplainability%E2%80%9D>

Clancy,C.Robbins, D., Ozgur E., Booker,Enos, K. (2023). *A Sensible Regulatory Framework for AI Security*. [online] MITRE. Available at: <https://www.mitre.org/newsinsights/publication/sensible-regulatory-framework-ai-security>.

Clarke, P. (2023). *Deutsche Bank eyes ‘game-changer’ AI in dealmaking unit*. [online] www.fn london.com. Available at: <https://www.fn london.com/articles/deutsche-bank-ai-dealmaking-unit-fabrizio-campelli-20230626> [Accessed 15 Aug. 2023].

Cloudflare (2022). *What is a DDoS attack?* [online] Cloudflare. Available at: <https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/>.

Cloudflare (2022). *What is a DDoS attack?* [online] Cloudflare. Available at: <https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/>.

Bank, E.C. (2023). Financial Stability Review, May 2023. www.ecb.europa.eu. [online] Available at: <https://www.ecb.europa.eu/pub/financial-stability/fsr/html/ecb.fsr202305~65f8cb74d7.en.html>.

[Basnet,P.](#)(2023). *Securing the Future: How AI Can Help Reduce Financial Fraud in Banking*. [online] Available at: <https://www.linkedin.com/pulse/securing-future-how-ai-can-help-reduce-financial-fraud-prem-basnet/> [Accessed 14 Aug. 2023].

Corporates.db.com. (n.d.). *Unleashing the potential of AI in securities services – Corporates and Institutions*. [online] Available at: <https://corporates.db.com/publications/White-papers-guides/unleashing-the-potential-of-ai-in-securities-services> [Accessed 16 Aug. 2023].

Council of Europe (2014). *History of Artificial Intelligence*. [online] Coe.int. Available at: <https://www.coe.int/en/web/artificial-intelligence/history-of-ai>.

Basnet,P.(2023). *Securing the Future: How AI Can Help Reduce Financial Fraud in Banking*. [online] Available at: <https://www.linkedin.com/pulse/securing-future-how-ai-can-help-reduce-financial-fraud-prem-basnet/> [Accessed 14 Aug. 2023].

Craig,P. (2019). *How to trust the machine: using AI to combat money laundering*. [online] Available at: https://www.ey.com/en_uk/trust/how-to-trust-the-machine--using-ai-to-combat-money-laundering.

Delaware. (n.d.). *AI transforms operational efficiency - delaware / a.i.* [online] Available at: <https://www.delaware.ai/core-processes/ai-quality-efficiency-operations> [Accessed 15 Aug. 2023].

Deloitte United Kingdom. (2018). *Robotic Process Automation | What Is RPA Technology? | Deloitte UK*. [online] Available at: <https://www2.deloitte.com/uk/en/pages/innovation/solutions/robotic-process-automation.html>.

Deutsche Bank website.(n.d.). *History*. [online] Available at: https://www.db.com/who-we-are/history/index?language_id=1&kid=history.redirect-en.shortcut.

Dictionary.cambridge.org. (n.d.). *deepfake*. [online] Available at:<https://dictionary.cambridge.org/dictionary/english/deepfake>.

Dupire, C. (2022). *The Global Facility steps forward – fighting money laundering and terrorist financing in the age of Covid*. [online] EU AML/CFT Global Facility. Available at: <https://www.global-amlcft.eu/the-global-facility-steps-forward-fighting-money-laundering-and-terrorist-financing-in-the-age-of-covid/#:~:text=Crime%20and%20money%20laundering%20did> [Accessed 11 Jul. 2023].

Eads,A.(2023). *How To Calculate the Mean (With Examples)*[online] Available at: <https://www.indeed.com/career-advice/career-development/how-to-calculate-the-mean>.

European Banking Authority. (2023). *The EBA publishes follow-up Report on the use of machine learning for internal ratings-based models*. [online] Available at: <https://www.eba.europa.eu/eba-publishes-follow-report-use-machine-learning-internal-ratings-based-models> [Accessed 23 Aug. 2023].

European Central Bank (2019). *The revised Payment Services Directive (PSD2)*. [online] European Central Bank. Available at: https://www.ecb.europa.eu/paym/intro/mip-online/2018/html/1803_revisedpsd.en.html.

European Central Bank (2019). *The revised Payment Services Directive (PSD2)*. [online] European Central Bank. Available at: https://www.ecb.europa.eu/paym/intro/mip-online/2018/html/1803_revisedpsd.en.html.

European Commission (2023). *A European approach to Artificial intelligence | Shaping Europe’s digital future*. [online] digital-strategy.ec.europa.eu. Available at: <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence>.

European-Union website. (n.d.). *European Central Bank (ECB) | European Union*. [online] Available at: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-central-bank-ecb_en#:~:text=The%20ECB%20works%20with%20the [Accessed 11 Jul. 2023].

European-Union website. (n.d.). *European Central Bank (ECB) | European Union*. [online] Available at: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-central-bank-ecb_en#:~:text=The%20ECB%20works%20with%20the [Accessed 11 Jul. 2023].

FCA. (2023). *Account information and payment initiation services*. [online] Available at: <https://www.fca.org.uk/consumers/account-information-payment-initiation-services> [Accessed 14 Aug. 2023].

Finance Digest website . (2023). *The future of artificial intelligence in banking and finance*. [online] Available at: <https://www.financedigest.com/the-future-of-artificial-intelligence-in-banking-and-finance.html> [Accessed 15 Aug. 2023].

Financial IT. (2023). *How AI Is Transforming the Financial Services Industry*. [online] Available at: <https://financialit.net/blog/ai-financialservices/how-ai-transforming-financial-services-industry#:~:text=Current%20State%20of%20AI%20in> [Accessed 14 Aug. 2023].

Finextra Research. (2023). *Generative AI: Why data protection needs to be emphasised*. [online] Available at: <https://www.finextra.com/the-long-read/736/generative-ai-why-data-protection-needs-to-be-emphasised#:~:text=Where%20financial%20institutions%20use%20generative> [Accessed 14 Aug. 2023].

Fripp, C. (2022). *New phishing scams targeting your bank account*. [online] Komando.com. Available at: <https://www.komando.com/money/bank-phishing-scams/837195/> [Accessed 16 Aug. 2023].

GOV.UK. (n.d.). *Government Cyber Security Strategy: 2022 to 2030 (HTML)*. [online] Available at: <https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030/government-cyber-security-strategy-2022-to-2030-html>.

Government of Canada, S.C. and Government of Canada, S.C. (2002). *Statistics: Power from Data! Calculating the mode*. [online] www150.statcan.gc.ca. Available at: <https://www150.statcan.gc.ca/n1/edu/power-pouvoir/ch11/mode/5214873-eng.htm>.

GSAM website. (n.d.). *Goldman Sachs Asset Management - Homepage*. [online] Available at: <https://www.gsam.com/content/gsam/global/en/homepage.html>.

Haricharan (2023). *Generative AI use cases in the Finance industry*. [online] Saxon. Available at: <https://saxon.ai/blogs/infusing-generative-ai-into-autonomous-finance/> [Accessed 23 Jul. 2023].

Harrison, P.J. (2021). *Wipro: Why are Financial Services a Prime Target for Cybercrime?* [online] The Fintech Times. Available at: <https://thefintechtimes.com/wipro-why-are-financial-services-a-prime-target-for-cybercrime/>.

Heimdal Security Blog. (2021). *Most Dangerous Financial Malware and How to Stay Safe*. [online] Available at: <https://heimdalsecurity.com/blog/banking-malware-trojans/>.

Heywood,D. (2023). *The UK's approach to regulating AI*. [online] Available at: <https://www.taylorwessing.com/en/interface/2023/ai---are-we-getting-the-balance-between-regulation-and-innovation-right/the-uks-approach-to-regulating-ai>.

Holmes,M.(2017).*How AI can help advisers with MiFID II*.Available at:[How AI can help advisers with Mifid II - FTAdviser.com](https://www.ftadviser.com/how-ai-can-help-advisers-with-mifid-ii/)

HSBC UK.(n.d).Our Privacy Notice 2 Contents. Available at: <https://www.hsbc.co.uk/content/dam/hsbc/gb/pdf/privacy-notice-full.pdf>.

HSBC. (2021). *Phishing Attacks | Things to Remember | Online Security | HSBC*. [online] Available at: <https://www.hsbc.com.tr/en/direct-banking/digital-banking/online-security/phishing>.

HSBC. (n.d.). *Our history | HSBC Holdings plc*. [online] Available at: <https://www.hsbc.com/who-we-are/our-history#:~:text=In%20March%201865%2C%20HSBC%20opened>.

Hussain, M. (2023). *Council Post: The Future Of Data And AI In The Financial Services Industry*. [online] Forbes. Available at: <https://www.forbes.com/sites/forbestechcouncil/2023/02/27/the-future-of-data-and-ai-in-the-financial-services-industry/?sh=7e6f59a23a00> [Accessed 24 Aug. 2023].

Hertz, L. (2023). *The Rise Of AI In The Banking And Finance Industry: Use Cases And Applications*. [online] Medium. Available at: <https://becominghuman.ai/the-rise-of-ai-in-the-banking-and-finance-industry-use-cases-and-applications-abfc3bd25c3c>.

IBM (2023). *What is Machine Learning?* [online] www.ibm.com. Available at: <https://www.ibm.com/topics/machine-learning>.

IBM (n.d.). *Customer experience consulting*. [online] Available at: https://www.ibm.com/consulting/customerexperience?utm_content=SRCWW&p1=Search&p4=43700067979438130&p5=e&gclid=CjwKCAjwxOymBhAFEiwAnodBLFdkgj1XSfcpq7pWptaXyzQiTlILPFXXIfqs9obv9jOtiKABt5gqTxoC-V0QAvD_BwE&gclsrc=aw.ds [Accessed 15 Aug. 2023].

Information Commissioner's Office (2018). *Essential guide to the General Data Protection Regulation (GDPR). Guide to the General Data Protection Regulation (GDPR)*. [online] doi:<https://doi.org/10.1211/pj.2017.20203048>.

Jeffers, J. (2023). *Fraud Detection in Banking Using Machine Learning*. [online] Security Boulevard. Available at: <https://securityboulevard.com/2023/04/fraud-detection-in-banking-using-machinelearning/#:~:text=Machine%20learning%20algorithms%20can%20analyze%20vast%20amounts%20of%20transactional%20data>.

Knowles, M. (2021). *Cybersecurity Risk Management: Frameworks, Plans, & Best Practices*. [online] Hyperproof. Available at: <https://hyperproof.io/resource/cybersecurity-risk-management-process/>.

KPMG. (2021). *Artificial Intelligence in Risk Management - KPMG United Arab Emirates*. [online] Available at: <https://kpmg.com/ae/en/home/insights/2021/09/artificial-intelligence-in-risk-management.html>.

Kushner, A. (2023). *Artificial Intelligence in Procurement*. [online] Approve.com. Available at: <https://www.approve.com/blog/artificial-intelligence-in-procurement/>.

Lavine, R. (2023). *Deutsche Bank zeroes in on AI investments*. [online] Global Venturing. Available at: <https://globalventuring.com/corporate/europe/deutsche-bank-ai-cvc-strategy/> [Accessed 16 Aug. 2023].

Leonardi, P. (2023). *The Digital Mindset: What It Really Takes to Thrive in the Age of Data, Algorithms, and AI - Book - Faculty & Research - Harvard Business School*. [online] Available at: <https://www.hbs.edu/faculty/Pages/item.aspx?num=62260>.

Leonards, A. (2023). *Deutsche Bank fined \$186m for AML failures*. [online] FStech. Available at: https://www.fstech.co.uk/fst/Deutsche_Bank_Fined_186m_For_AML_Failures.php [Accessed 15 Aug. 2023].

Maurer, T. and Nelson, A. (2021). *The Global Cyber Threat to Financial Systems – IMF F&D*. [online] www.imf.org. Available at: <https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm>.

Mckinsey (2021). *Global Banking Practice Building the AI bank of the future*. [online] Available at: <https://www.mckinsey.com/~media/mckinsey/industries/financial%20services/our%20insights/building%20the%20ai%20bank%20of%20the%20future/building-the-ai-bank-of-the-future.pdf>.

- Mejia, N. (2020). *Artificial Intelligence at HSBC - Internal Products and Investments*. [online] Emerj. Available at: <https://emerj.com/ai-sector-overviews/artificial-intelligence-at-hsbc/>.
- Metcalf-Dennis, N. (n.d.). *Process Optimisation: 5 Key Areas To Focus On | DocTech*. [online] www.doctech.co.uk. Available at: <https://www.doctech.co.uk/blog/process-optimisation-5-key-areas-to-focus-on-doctech> [Accessed 15 Aug. 2023].
- Milne, A. (2021). *The Top Financial Services Cyber Threats | Field Effect*. [online] Field Effect Software Inc. Available at: <https://fieldeffect.com/blog/financial-services-cyber-threats/>.
- Mixson, E. (2021). *AI at HSBC PART 1: Can AI Be Used To Promote Trust & Accountability?* [online] AI, Data & Analytics Network. Available at: <https://www.aidataanalytics.network/data-governance/articles/ai-at-hsbc-part-1-can-ai-be-used-to-promote-trust-accountability>.
- Monti, M. (2023). *Is Europe heading for another banking crisis?* [online] EUROPP. Available at: <https://blogs.lse.ac.uk/euoppblog/2023/03/30/is-europe-heading-for-another-banking-crisis/>.
- NatWest bank. (n.d.). *Turning the future of banking into a reality*. Available at: [The-future-of-banking \(PUBLIC\).pdf \(rbs.com\)](#).
- Naz, Z. (2023). *Cybersecurity in Banking Sector: Importance, Threats, Challenges*. [online] www.knowledgehut.com. Available at: <https://www.knowledgehut.com/blog/security/cyber-security-in-banking>.
- Newsletter on artificial intelligence and machine learning. (2022). www.bis.org. [online] Available at: https://www.bis.org/publ/bcbs_nl27.htm.
- NICE Systems. (n.d.). *What is Intelligent Process Automation (IPA)? | NICE*. [online] Available at: <https://www.nicerpa.com/rpa-guide/what-is-intelligent-process-automation-ipa/#:~:text=IPA%20is%20the%20product%20of> [Accessed 24 Aug. 2023].
- Nordlayer.com. (n.d.). *What is Network Encryption? | NordLayer Learn*. [online] Available at: <https://nordlayer.com/learn/network-security/network-encryption/#:~:text=Network%20encryption%20applies%20to%20network> [Accessed 22 Aug. 2023].
- OECD (2021). *Artificial Intelligence, Machine Learning and Big Data in Finance Opportunities, Challenges and Implications for Policy Makers*. [online] OECD. Available at: <https://www.oecd.org/finance/financial-markets/Artificial-intelligence-machine-learning-big-data-in-finance.pdf>.
- PayPal Newsroom. (2023). *PayPal Ventures Invests in Finanzguru*. [online] Available at: <https://newsroom.paypal-corp.com/2023-04-04-PayPal-Ventures-Invests-in-Finanzguru> [Accessed 16 Aug. 2023].
- Precisely. (2023). *Two Factor Authentication (2FA)*. [online] Available at: <https://www.precisely.com/glossary/two-factor-authentication-2fa>.
- Queensland Brain Institute. (2019). *History of Artificial Intelligence*. [online] Available at: <https://qbi.uq.edu.au/brain/intelligent-machines/history-artificial-intelligence>.
- S&P Global. (2023). *Europe's 50 largest banks by assets, 2023*. [online] Available at: <https://www.spglobal.com/marketintelligence/en/news-insights/research/europes-50-largest-banks-by-assets-2023> [Accessed 11 Jul. 2023].

Sacred Heart University Library (2020). *Research Guides: Organizing Academic Research Papers: Types of Research Designs*. [online] Sacredheart.edu. Available at: <https://library.sacredheart.edu/c.php?g=29803&p=185902>.

Saha, S. (2023). *How Deutsche Bank is Riding the Generative AI Wave*. [online] Analytics India Magazine. Available at: <https://analyticsindiamag.com/how-deutsche-bank-is-riding-the-generative-ai-wave/#:~:text=Deutsche%20Bank%27s%20Generative%20AI%20Voyage&text=Currently%2C%20the%20bank%20is%20globally> [Accessed 15 Aug. 2023].

Sangfor Technologies (2022). *Cyber-attacks on Banks Devastate the Financial Sector*. [online] SANGFOR. Available at: <https://www.sangfor.com/blog/cybersecurity/cyber-attacks-on-banks-devastate-financial-sector>.

Sayegh, E. (2023). *Potential For Devastation: The Impact Of A Cyberattack On The Banking System*. [online] Forbes. Available at: <https://www.forbes.com/sites/emilsayegh/2023/06/06/potential-for-devastation-the-impact-of-a-cyberattack-on-the-banking-system/?sh=2ca9c3361b45> [Accessed 23 Jul. 2023].

Shetty,P.(2022). *Artificial Intelligence is the Future of the Banking Industry — Are You Prepared for It?* [online] International Banker. Available at: <https://internationalbanker.com/technology/artificial-intelligence-is-the-future-of-the-banking-industry-are-you-prepared-for-it/>.

Statista. (2023). Artificial Intelligence market size 2030. [online] Available at: <https://www.statista.com/statistics/1365145/artificial-intelligence-market-size/#:~:text=Global%20artificial%20intelligence%20market%20size%202021%2D2030&text=Its%20value%20of%20nearly%20100>.

SymphonyAI Sensa-NetReveal. (2021). *Sensa™ AML: A Powerful Silver Bullet to Money Laundering*. [online] Available at: <https://www.netreveal.ai/news/symphony-ayasdiai-launches-sensa-a-pioneering-solution-for-aml-and-financial-crime-detection-to-thwart-money-laundering-activities/> [Accessed 16 Aug. 2023].

SymphonyAI Sensa-NetReveal. (n.d.). *HSBC Fights Back Against Financial Crime Actors with AI*. [online] Available at: <https://www.netreveal.ai/resources/blogs/anti-moneylaunderinghsbc/>.

Szczepański, M. (2019). *Economic impacts of artificial intelligence (AI)*. [online] European Parliament. Available at: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/637967/EPRS_BRI\(2019\)637967_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/637967/EPRS_BRI(2019)637967_EN.pdf)

Tanant, F. (2018). *How to Combine Machine Learning and Human Intelligence for Better Fraud Detection*. [online] SEON. Available at: <https://seon.io/resources/fraud-detection-with-machine-learning/>.

Taylor, S. (2022). *Mean*. [online] Corporate Finance Institute. Available at: <https://corporatefinanceinstitute.com/resources/data-science/mean/>.

Thomas, M. (2023). *The future of artificial intelligence*. [online] Built In. Available at: <https://builtin.com/artificial-intelligence/artificial-intelligence-future>.

Thormundsson, B. (2023). *Artificial Intelligence market size 2030*. [online] Statista. Available at: <https://www.statista.com/statistics/1365145/artificial-intelligence-market-size/#:~:text=According%20to%20Next%20Move%20Strategy>.

Tobin,J.(2023). *Artificial intelligence: Development, risks and regulation*. Available at: [Artificial intelligence: Development, risks and regulation - House of Lords Library \(parliament.uk\)](#).

Toronto Centre,(2022).*Supervisory Implications of Artificial Intelligence and Machine Learning*.Available.https://www.torontocentre.org/videos/Supervisory_Implications_of_AI_and_ML_FINAL.pdf [Accessed 11 Aug. 2023]

UNESCO (2022). *Ethics of artificial intelligence | UNESCO*. [online] www.unesco.org. Available at: <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics>.

University of Pennsylvania (n.d.). *Executive Education at The Wharton School - Executive Programs*. [online] Available at: <https://executiveeducation.wharton.upenn.edu/>.

Rijmenam, M.(2023). *Privacy in the Age of AI: Risks, Challenges and Solutions*. [online] Dr Mark van Rijmenam, CSP - The Digital Speaker | Strategic Futurist. Available at: <https://www.thedigitalspeaker.com/privacy-age-ai-risks-challenges-solutions/>.

Vejay L., Mitrani, A., Harned,Z.(2022). *Artificial intelligence: deepfakes in the entertainment industry*. [online] Available at: https://www.wipo.int/wipo_magazine/en/2022/02/article_0003.html.

Weiser, S. (2019). *Requirements of Trustworthy AI*. [online] FUTURIUM - European Commission. Available at: <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines/1.html#:~:text=significantly%20affects%20them.->.

Wilson, H.J. and Daugherty, P.R. (2019). *Collaborative Intelligence: Humans and AI Are Joining Forces*. [online] Harvard Business Review. Available at: <https://hbr.org/2018/07/collaborative-intelligence-humans-and-ai-are-joining-forces>.

Wordvice. (2023). *How To Present Study Limitations and Alternatives*. [online] Wordvice. Available at: <https://blog.wordvice.com/how-to-present-study-limitations-and-alternatives/>.

Workplace Health and Safety Queensland (2013). *Understanding safety culture*. [online] Available at: https://www.worksafe.qld.gov.au/data/assets/pdf_file/0024/19365/understanding-safety-culture.pdf.

www. *Understanding email fraud | Barclays*. [online] Available at: <https://www.barclays.co.uk/journal/email-payment-fraud/> [Accessed 22 Aug. 2023].

www.automationanywhere.com. (n.d.). *Optimize Efficiency with Business Process Automation | AutomationAnywhere.com*. [online] Available at: <https://www.automationanywhere.com/rpa/robotic-process-automation#:~:text=RPA%2C%20or%20Robotic%20Process%20Automation> [Accessed 24 Aug. 2023].

www.db.com. (2022). *Deutsche Bank Partners with NVIDIA to embed AI into Financial Services*. [online] Available at: <https://www.db.com/news/detail/20221207-deutsche-bank-partners-with-nvidia-to-embed-ai-into-financial-services#:~:text=Deutsche%20Bank%20and%20NVIDIA%20are>.

www.ibm.com. (n.d.). *Customer experience consulting*.

www.javatpoint.com. (n.d.). *Machine Learning Algorithms - Javatpoint*. [online] Available at: <https://www.javatpoint.com/machine-learning-algorithms>.

www.javatpoint.com. (n.d.). *What is Artificial Intelligence (AI)? Tutorial, Meaning - Javatpoint*. [online] Available at: <https://www.javatpoint.com/artificial-intelligence-ai>.

www.jpmorgan.com. (n.d.). *12 Tips for Mitigating Cyber Risk | JPMorgan Chase*. [online] Available at: <https://www.jpmorgan.com/insights/cybersecurity/ransomware/12-tips-for-mitigating-cyber-risk>.

www.ncsc.gov.uk. (n.d.). *Always back up your most important data*. [online] Available at: <https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/always-back-up-your-most-important-data>.

www.tripwire.com. (2022). *Artificial Intelligence, a new chapter for Cybersecurity?* [online] Available at: <https://www.tripwire.com/state-of-security/artificial-intelligence-new-chapter-cybersecurity>.

Wyman, O. (2019). *Artificial Intelligence Applications In Financial Services*. [online] www.oliverwyman.com. Available at: <https://www.oliverwyman.com/our-expertise/insights/2019/dec/artificial-intelligence-applications-in-financial-services.html>.

Yoskowitz, R. (2023). *Why Is Controlling Access to Data So Hard?* [online] Available at: <https://www.nullafi.com/blog-posts/why-is-controlling-access-to-data-so-hard> [Accessed 11 Aug. 2023].

Zendesk. (n.d.). *9 ways businesses use AI in customer service in 2023*. [online] Available at: <https://www.zendesk.co.uk/blog/ai-customer-service/#georedirect>. Analytics

Software & Solutions(2019). *What is Natural Language Processing?* [online] Available at: https://www.sas.com/en_gb/insights/analytics/what-is-natural-language-processing-nlp.html.

13.Appendix

Customer Perspectives on AI-Related Cyber Threats in the Banking System:
A Survey on Knowledge, Awareness, and Precautions

The following questionnaire aims to gather valuable insights regarding the knowledge, awareness, and perceptions of AI-related cyber threats in the banking system from customers' perspectives.

Your responses will contribute to a research study exploring how the European financial and banking sectors can leverage the potential of artificial intelligence to enhance operational efficiency while effectively addressing cybersecurity threats.

* Indicates required question

1. Are you familiar with the AI-Related Cyber Threats? *

Mark only one oval.

- ☐ Yes
☐ No
☐ Other: _____

2. Have you heard about phishing attacks leveraging AI for social engineering purposes? *

Mark only one oval.

- ☐ Yes
☐ No
☐ Other: _____

3. Are you aware of deepfake fraud, which involves impersonation and manipulation using AI-generated content? *

Mark only one oval.

- ☐ Yes
☐ No
☐ Other: _____

4. Are you familiar with the concept of malware and botnets powered by AI automation in cyber attacks? *

Mark only one oval.

- ☐ Yes
☐ No
☐ Other: _____

5. Are you aware of privacy concerns related to AI, such as data breaches and unauthorized access? *

Mark only one oval.

- ☐ Yes
- ☐ No
- ☐ Other:

6. How cautious are you when it comes to suspicious communications that may be attempts to exploit AI for cyber threats? *

Mark only one oval.

- ☐ Very cautious
- ☐ Somewhat cautious
- ☐ Not cautious at all

7. Do you use secure devices and networks when conducting financial transactions online? *

Mark only one oval.

- ☐ Yes, always
- ☐ Sometimes, depending on the circumstances
- ☐ No, not at all

8. How frequently do you monitor your accounts for any suspicious activity? *

Mark only one oval.

- ☐ Regularly, on a daily or weekly basis
- ☐ Occasionally, on a monthly basis
- ☐ Rarely, only when something seems amiss

9. How do you protect your personal information from potential AI-related cyber threats? (Select all that apply) *

Tick all that apply.

- ☐ Using strong and unique passwords
- ☐ Enabling two-factor authentication
- ☐ Being cautious about sharing personal information online
- ☐ Regularly updating security software on devices
- ☐ Other (please specify)

10. If you come across any suspicious activity related to AI-driven cyber threats, would you report it to your financial institution or the appropriate authorities? *

Mark only one oval.

- ☐ Yes, always
- ☐ Sometimes, depending on the severity of the activity
- ☐ No, never

11. In your opinion, what measures should financial institutions take to enhance operational efficiency while effectively addressing cybersecurity threats related to AI? (Please provide your suggestions and recommendations) *
