IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DIGITAL RISK MANAGEMENT IN BANKS AND THE INFLUENCE OF EMERGING TECHNOLOGIES

Nirooj Fidin

Senior Manager (IT)

Union Learning Academy – Digital Transformation,

Union Bank of India, Mumbai, India

Abstract: In the ever-evolving digital landscape, organizations face unprecedented challenges in managing risks associated with their digital assets and sensitive data. The integration of emerging technologies has transformed the business landscape, leading to complex and evolving risks with severe consequences. This research paper focuses on the banking sector, exploring the latest technologies and associated risks, while also delving into effective digital risk management practices.

The paper provides a comprehensive overview of the digital risk landscape, including strategies and best practices employed by organizations to manage digital risk effectively. Challenges faced by organizations in managing digital risks, such as evolving cyber threats and data protection compliance complexities, are discussed.

To comprehensively understand digital risk management, a combination of qualitative and quantitative approaches is used, including a literature review of relevant studies and the impact of emerging technologies on risk management. The study emphasizes the importance of robust risk management practices and continuous adaptation to evolving threats and regulations in ensuring secure and successful digital initiatives in the banking industry.

Overall, effective digital risk management is crucial in the rapidly evolving banking landscape. By implementing robust mitigation measures, banks can leverage emerging technologies to enhance services and customer experiences while safeguarding data and ensuring regulatory compliance. Proactively addressing digital risks will pave the way for a secure and prosperous future for the banking industry.

Index Terms **- Artificial Intelligence, Machine Learning, Blockchain, Internet of Things, Open Banking, Hyper Personalized banking, Cloud banking, Robotic process automation, Quantum Computing, Metaverse, Emerging Technologies, Cyber Security, Digital Risk.**

1. INTRODUCTION

In the dynamic and rapidly evolving digital era, organizations are confronted with unprecedented challenges when it comes to managing the various risks applicable to their digital assets, sensitive data, and critical. Integration of new and emerging technologies into existing operations has a penetrative effect on the business as a whole due to the interconnected nature of today's business along with exponential growth of data. Collectively, these have given rise to complex and evolving risks that can have severe consequences for the business and its stakeholders. Therefore, effectively managing digital risk has emerged as a critical function for organizations operating seeking to enhance their digital infrastructure.

Managing digital risk entails a diverse and holistic set of practices and strategies designed to identify, assess, mitigate, and respond to the constantly evolving landscape of cyber threats, vulnerabilities, and data breaches.

2. OBJECTIVES

The objective of this research is to delve into the latest and emerging technologies that are currently being implemented or can be implemented in the banking system, the associated risks that come about due to their implementation and identify the challenges they face in safeguarding their digital assets effectively.

Whenever a bank undergoes a digital transformation journey, the existing risk management and security practices require to be revamped and reworked in order to accommodate and mitigate the new risks brought about by the adoption the new technology. However, at present many banks focus initially on how to be more digital—move at speed, use data to make decisions, respond rapidly and think about risk and compliance quite late. In order to keep up with emerging technologies and its adoption in the banking sector, digital risk management is essential and it is imperative for the risk management process to be able to adapt and be able to mitigate the risks associated with new technologies.

Digital risk management in banking involves identifying, assessing, and mitigating risks associated with digital technologies and channels. The use of digital technologies, such as mobile banking, online banking, and electronic payments, has significantly transformed the banking industry, but it has also brought new risks and challenges. Similarly as new age technologies like blockchain, cloud computing, IoT, Artificial Intelligence etc. are in vogue and on the verge of being adopted in the banking system, the risk management process has to be overhauled accordingly.

3. SCOPE AND STRUCTURE

This research paper will begin by providing an overview of the digital risk landscape, highlighting the key factors that have contributed to the emergence and evolution of digital risks. It will then delve into the various strategies and best practices employed by organizations to manage digital risk effectively.

Next, the paper will discuss the challenges and obstacles that organizations face in managing the various digital risks. This includes the constantly evolving nature of cyber threats, the complexities of compliance with data protection regulations, the growing sophistication of attackers, and the emergence of new tools and technologies.

4. METHODOLOGY

Digital risk management in banking involves various processes, such as risk identification, risk assessment, risk mitigation, and risk monitoring. Banks need to identify the potential risks associated with their digital channels, such as cyber-attacks, data breaches, identity theft, and fraud. They also need to assess the likelihood and impact of these risks and implement appropriate measures to mitigate them.

The research aims to venture out and collect the various risk management measure that can be imbibed into the current processes and also determine how these new technologies will impact the thoughts and conditioning of the individuals designing the process.

The research design adopts a versatile approach in order to provide a comprehensive understanding of the management of digital risk. As we are going to delve into emerging technologies, due the novelty of these technologies it is deemed that the research design combine qualitative and quantitative approaches to capture both subjective insights and objective data related to digital risk management strategies, practices, and challenges. Data collection would involve sourcing through multiple sources with varied weightage across each source.

5. LITERATURE REVIEW

The literature review involves a systematic analysis of academic journals, conference papers, and relevant books focusing on digital risk management as well as emerging technologies. Key academic databases, such as research gate and Google Scholar, were utilized to identify scholarly publications in the field.

Furthermore, the literature review identified key challenges faced by organizations in managing digital risk. The works of Jones (2017) and Kim et al. (2019) emphasized the growing complexity of cyber threats and the need for continuous monitoring and adaptation of risk management strategies. These studies also emphasized the role of employee education and awareness programs in mitigating human-related risks.

Sunil Mithas, Zhi-Long Chen, Terence J.V. Saldanha and Alysson De Oliveira Silveira(2022) identified key influences areas of Artificial Intelligence, Blockchain, Advanced Robotics, Autonomous Systems and Internet of Things upon the supply chain management and the operational aspects of an organization. They elaborated the disruptive effects these technologies have on existing bottlenecks and how certain business functions are overhauled.

Oscar Rodríguez-Espíndola, Soumyadeb Chowdhury, Prasanta Kumar Dey, Pavel Albores and Ali Emrouznejad (2022) theorizes that regulatory support can make a significant difference in the perception of employees and user acceptance of emerging technologies and the respective response towards the associated digital risks. Investing in organisational resilience can enhance the willingness for technology adoption for risk management. Organisations aware of vulnerabilities and the potential impact of disruptions value the prospective benefits of disruptive technologies and can leverage capabilities such as flexibility and adaptability to support the implementation of technologies.

Phillip Williams, Indira Kaylan Dutta, Hisham Daoud and Magdy Bayoumi (2022) talks about how IoT has opened up unlimited possibilities for serving society but there has also been challenges in regards to cyber threats and attacks due to constraints of devices such as power, memory, are etc. Additionally, this research outlines how emerging technologies such as machine learning and blockchain are integrated in IoT, challenges resulted from this integration, and potential solutions to these challenges.

María M. Feliciano-Cestero, Nisreen Ameen, Masaaki Kotabe, Justin Paul and Mario Signoret (2023) highlights key issues related to digital transformation at the individual, firm, and macro (international) levels and its impact on firms' internationalization process. They analyze the human and non-human impact of digital transformation that can either allow or threaten it and their impact on firms' internationalization.

6. DATA COLLECTION

The implementation of new digital technology in banking has opened up avenues to improve customer experience, generate additional revenue by offering new and expanded services, and streamline transaction processing for greater efficiency and cost-effectiveness. Nonetheless, alongside these opportunities, digital technology has also altered existing risks and frequently introduced novel ones for banks, customers, and other parties involved.

For example, introduction of MICR technology had a significant impact on the speed of processing checks and freed up human resources, increasing revenues and reducing expenses. However, it changed the risk of misrouted and misposted cheques from a discreet event associated with human, clerical error, into a systemic risk associated with the threat of malicious and accidental computer programming errors. These systemic errors resulted in entire batches of hundreds or thousands of checks being misrouted, disrupting the bank's liquidity and introducing the need, on occasion, to correct much larger numbers of misrouted checks and associated customer compensation claims. Thus, risk was transformed from solely being associated with low-velocity operating errors to high-velocity risk, with significant financial and regulatory ramifications.

Digital transformation often brings about changes in the nature of existing risks and introduces new and unforeseen risks. The key characteristics of digital risk in the Indian banking sector are as follows:

1. **Digital Risk Emerging due to Rapid Implementation**: Whenever a bank introduces new or modified digital products, services, business processes, or assets, it gives rise to digital risk. This includes third-party digital technology provided to the bank. Many banks rush to implement and adopt new technologies in order to gain first mover advantage and attract new and savvy customers. Regulations for these technologies may not exist initially and can emerge later due to perceived harm or unexpected outcomes. Eg: When bitcoin was introduced, many startups were founded that enabled bitcoin transactions and trading. However, due to its volatile nature, bitcoin is losing traction among users.

2. **Amplified Impact of Inherent Risk**: With manual processing, errors and fraud tend to be isolated to individual transactions. However, in automated transaction processing, any errors or fraud introduced can spread across multiple transactions, increasing the impact of inherent risks. Eg: The global financial crisis of 2008, also known as the Great Recession, was a severe economic downturn that affected countries worldwide. The crisis originated in the United States and was primarily triggered by the collapse of the housing market and the subprime mortgage crisis. The financial crisis demonstrated how the interconnectedness of the global financial system and the amplification of inherent risks in the banking and financial sectors could lead to a widespread economic collapse.

3. **Broader, Complex Threat Sources**: Banks implementing process automation require both digital technology assets and skilled human resources. Outsourcing technology-related activities to third parties is common, but banks remain responsible for managing associated risks, especially vendor driven. Ensuring identity and access management can be challenging, and unauthorized access can lead to fraud, financial loss, privacy breaches, compliance violations, financial reporting irregularities, and reputational damage.

4. **Interconnectedness and Technology Hubs**: Processes interconnected through common technology hubs, such as servers or telecommunication routers, are susceptible to spreading attacks. Banks may struggle to fully understand their technology interconnections, assess associated risks, and allocate resources effectively. Interconnectedness exposes banks to frauds across multiple channels, where attackers manipulate multiple communication channels to achieve their fraudulent objectives. Additionally, publicly facing technologies, like those accessible via the internet, are vulnerable to malicious attacks. For eg: In June 2017, a massive cyberattack targeted businesses and organizations worldwide, primarily in Ukraine but with significant collateral damage globally. The attack was initially disguised as ransomware and dubbed "Petya" or "NotPetya" due to its resemblance to the Petya ransomware that had appeared earlier. The interconnectedness of the global technology ecosystem played a crucial role in the rapid and far-reaching spread of the NotPetya malware. The attackers exploited vulnerabilities in widely used software and leveraged technology hubs to distribute the malware to multiple organizations simultaneously.

5. **Access Restrictions and Governance**: Restricting access to technology user interfaces and the technology itself to authorized individuals based on their roles and responsibilities is crucial for ensuring sound governance, internal control, and preventing errors and fraud.

6. **Increased Velocity of Risk**: Automated processes can lead to rapid material incidents or losses compared to manual processes. The speed at which digital risk can emerge renders traditional non-digital risk control methods less effective. For example, in December 2020, it was revealed that a sophisticated cyberattack had been carried out on SolarWinds, a major IT management software company. The attackers compromised SolarWinds' software development process and inserted malicious code into their software updates, specifically the Orion platform. Orion is widely used by organizations, including government agencies and private companies, to monitor and manage their IT infrastructure. The cyberattack's primary threat was the rapid and stealthy distribution of the malicious software updates to SolarWinds' customers. Since the updates were digitally signed by SolarWinds and considered legitimate, they were quickly distributed and installed on thousands of networks worldwide, without raising immediate suspicions.

7. **Consumer Privacy**: With digital transformation in banking, handling consumer information raises significant concerns about consumer privacy. While comprehensive privacy legislation is still evolving in India, banks must govern their data and manage privacy risks in compliance with existing regulations and any emerging privacy laws.

8. **Unknown, Emerging, and Transformed Regulations**: Innovating banks in India often encounter a lack of regulations governing their new initiatives. Anticipating future regulations, such as privacy regulations, is possible to some extent. However, certain areas, like the specific use of artificial intelligence (AI), currently lack comprehensive regulations. Moreover, existing regulations transform as banking operations shift digitally, requiring banks to adapt their governance processes accordingly.

9. **Third-Party Risk**: Due to resource constraints, many Indian banks rely on third parties, including cloud providers, for digital products, services, and support systems. While outsourcing is an option, the associated risks cannot be outsourced. Banks must understand and effectively manage the digital risks associated with outsourcing, particularly considering Indian banking regulations. For example, In July 2019, Capital One, one of the largest banks in the United States, experienced a significant data breach that exposed the personal information of over 100 million customers and applicants. The data breach was a result of a third-party vendor's security vulnerability. The attacker gained unauthorized access to Capital One's customer data stored on Amazon Web Services (AWS) servers, which were managed by a third-party cloud service provider.

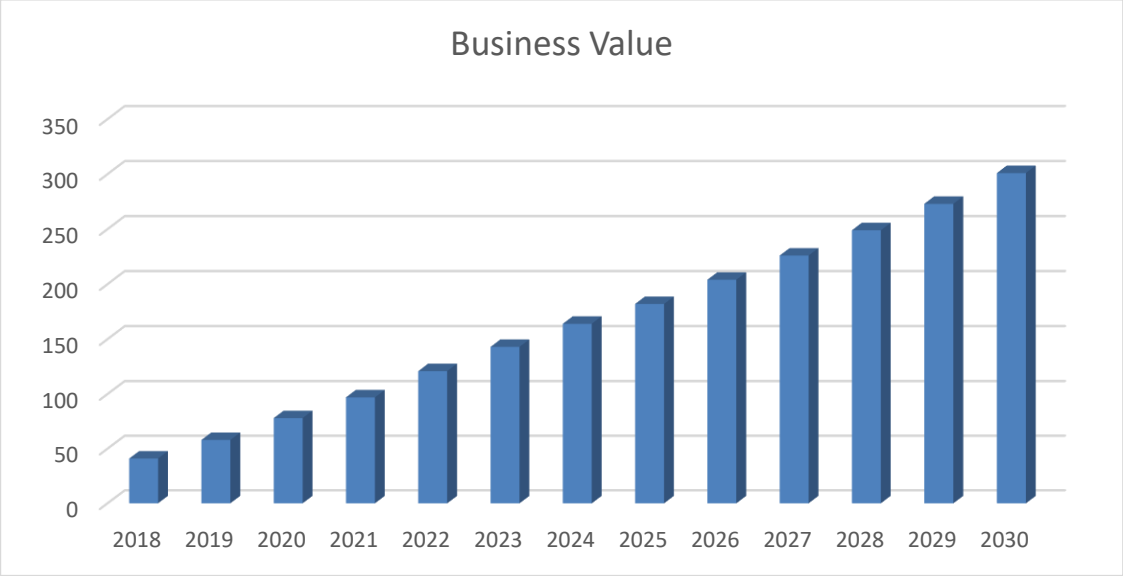
These characteristics highlight the complex landscape of digital risk in the Indian banking industry, necessitating robust risk management practices and continuous adaptation to evolving threats and regulations. Indian banks must prioritize digital risk management to ensure the secure and successful implementation of digital initiatives.

Some of the latest emerging technologies in the banking and financial sector are:

1. **Artificial Intelligence and Machine Learning**

AI enables banks to provide high-quality banking services to their customers and save operating costs. AI-powered tools, such as virtual assistants and chatbots, automate customer service interactions. Additionally, they provide customers with account information and resolve account-related queries. AI-based biometrics detect fraud and improve security, as well as enhance AML applications and KYC checks. Further, machine learning (ML) algorithms power alternate credit score modeling that aids banks in making better lending decisions. Computer vision-enabled tools also simplify document analysis, which assists banks in customer onboarding and compliance management. Moreover, AI analyzes massive financial datasets to improve risk assessment and financial forecasting, improving investing decisions.

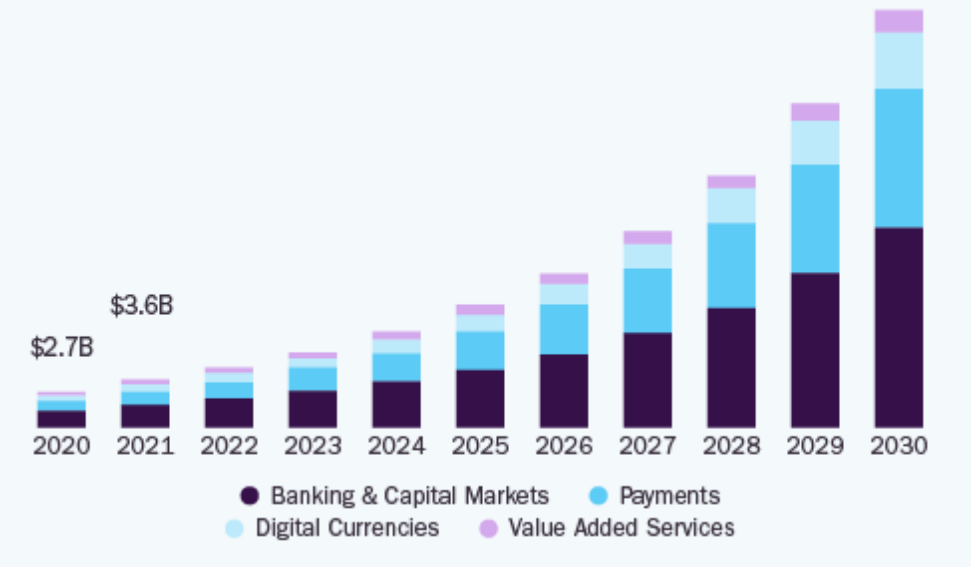
Fig 1: Business growth projection of AI in banking



2. **Open Banking**

Open banking connects non-banking financial companies (NBFCs) and banks to provide customers with custom and more accessible financial services. Banking application programming interfaces (APIs) enable third-party developers to securely access customer financial data without compromising data compliance. Open banking also includes account aggregators that allow customers to manage all their banking accounts through a single platform. Additionally, APIs from banks allow NBFCs to integrate banking functionality into their apps and services. This embedded banking enables NBFCs to verify customer information automatically, reducing the need for manual verification and accelerating customer verification. Moreover, open banking enables banking-as-a-service (BaaS) that allows banks to reach new customers through third parties and increase their revenue.

Fig 2: Business growth projection of Open Banking and allied services



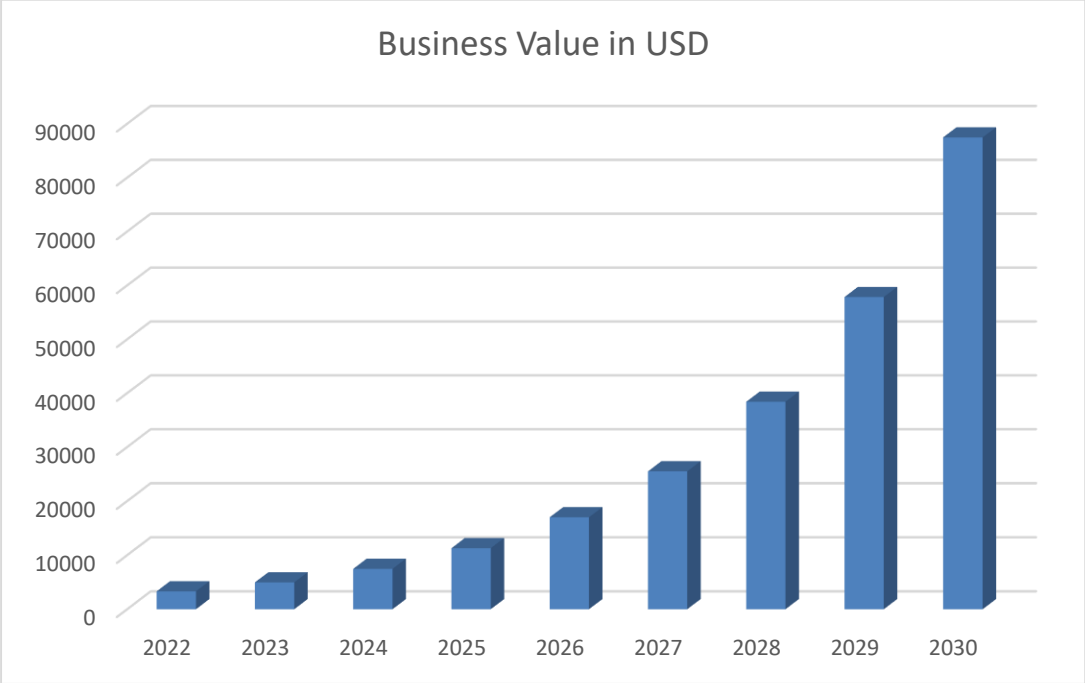
3. **Hyper-Personalized Banking**

Providing a personalized banking experience improves customer retention. That is why banks now leverage various strategies and technologies, such as buy now pay later (BNPL), omnichannel banking, and financial advisory tools, to tailor their offerings. For instance, omnichannel banking provides a unified, customer-centric view of their financial information while allowing them to interact with banks via multiple channels. Additionally, wealth management and financial advisory tools provide customized advice and investment guides, improving investor and customer satisfaction. Banks thus leverage AI and machine learning to provide such real-time personalized financial recommendations.

4. **Blockchain**

Blockchain provides tamper-proof records of all financial transactions and improves transactional transparency and security. Further, it improves trade efficiency through transaction automation as well as streamlines manual and paper-based operations. Smart contracts automate financial transactions and improve the performance of financial contracts. They also eliminate the need for intermediaries and enable peer-to-peer (P2P) payments. This greatly enhances the speed and efficiency of transactions, especially cross-border payments. Moreover, decentralized finance leverages blockchain to make financial services more accessible while lowering transaction fees.

Fig 3: BFSI market size of Blockchain



5. **Immersive Technologies and Metaverse**

Immersive technologies, such as virtual reality (VR) and augmented reality (AR), offer banks exciting opportunities to enhance customer experiences and improve internal operations. By creating virtual branches, offering digital customer service, and providing engaging financial education through VR and AR, banks can deliver personalized services and streamline employee training. Additionally, immersive technologies can enable virtual property tours and showcase investment opportunities to customers, fostering deeper engagement and understanding.

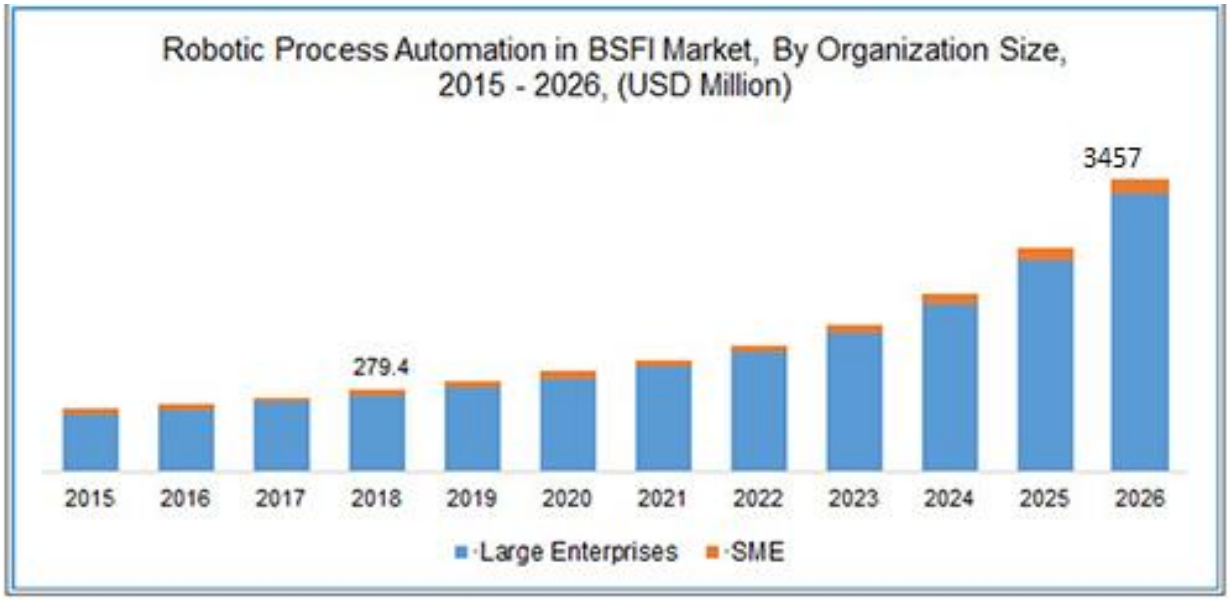
The metaverse, a collective virtual shared space combining AR, VR, and the internet, presents new horizons for the banking industry. Banks can host virtual events, create digital marketplaces for assets like virtual currencies and NFTs, and offer secure digital identities in the metaverse. Moreover, integrating with decentralized finance platforms within the metaverse allows banks to extend their reach to a global digital audience and explore innovative financial products. While embracing these technologies, banks must prioritize data privacy, cybersecurity, and regulatory compliance to ensure seamless and secure experiences for customers and employees alike. By leveraging immersive technologies and embracing the metaverse, banks can elevate their offerings, foster innovation, and stay ahead in the ever-evolving digital banking landscape.

By leveraging immersive technologies, banks thus ensure a more engaging customer experience to increase customer satisfaction and loyalty.

6. **Banking Process Automation**

Banking Process Automation involves using technology and software to streamline and optimize various banking operations, reducing manual intervention and increasing efficiency. It includes workflow automation, customer service automation, document processing, risk and compliance automation, fraud detection, loan origination, and payment processing. The benefits of banking process automation include improved efficiency, enhanced accuracy, cost savings, better customer experience, and scalability. However, challenges such as integration complexity, data security concerns, training, change management, and regulatory compliance need to be addressed for successful implementation.

Fig 4: BFSI market size of RPA



7. **Cloud Banking**

For many banks, cloud banking is transforming their cost-efficiency and allowing them to create new experiences for their clients while maintaining the traditional model in place. In the cloud, banks are able to synchronize the enterprise and break down operational and data silos across customer care, finance, risk, and other areas of the business.

8. **Quantum Computing**

With traditional computing, processing huge amounts of data is resource and time-intensive. Quantum computing solves this problem by offering faster, more efficient, and more secure computing. It assists banks in optimizing their portfolios and making accurate financial predictions. Companies like Google and IBM are thus developing cost-effective quantum computers. They assist banks in derivative pricing and improving their cybersecurity programs. It's also important to note that quantum computing is still in its early stages, and practical, large-scale quantum computers suitable for banking applications are yet to be realized. The development of quantum-safe encryption is also a critical aspect to ensure the security of financial data and transactions in a quantum-powered future. As the technology progresses, we can expect to see more research, experimentation, and potential applications of quantum computing in the banking industry.

7. FINDINGS AND RECOMMENDATIONS

Based on the information collected, the technologies have been analyzed and some of the digital risks that these technologies are susceptible to are explored below. In addition to identifying these risks, some mitigation measures that can be undertaken have been suggested based on the information and knowledge gained during the scope of this research. Decision to adopt and execute the relevant mitigation measure is up to the cybersecurity team of the bank.

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

AI and ML offer numerous use cases that can aid the banking sector's growth and development. Some applications include:

- **Fraud Detection:** AI and ML algorithms can analyze vast transaction data to identify unusual patterns and detect potential fraudulent activities.
- **Customer Service:** AI-powered chatbots provide instant customer support, enhancing customer experience and reducing response times.
- **Risk Management:** AI can be used for credit risk assessment, predicting loan defaults, and optimizing portfolio management.
- **Personalized Banking:** ML algorithms analyze customer behaviour and preferences to offer personalized product recommendations and customized services.
- **AML and KYC:** AI assists in automating AML and KYC processes, streamlining customer onboarding and transaction monitoring for suspicious activities.

- **Trading and Investment:** AI-powered algorithms analyze market data, predict trends, and make informed investment decisions.

Risks and Mitigation Measures:

- **Bias and Fairness Risks:** AI and ML algorithms can be biased, leading to unfair or discriminatory treatment of certain customer groups.
    - **Mitigation:** These can be mitigated by investing in diverse datasets, regularly auditing the algorithms for fairness and transparency, and involve diverse teams in algorithm development to address potential bias. One should also implement guidelines for ethical AI use and avoid using AI in ways that may lead to unfair treatment of certain customer groups.

- **Model Robustness Risks:** AI and ML models may lack robustness and could be susceptible to adversarial attacks or unforeseen inputs.
    - **Mitigation:** It can be averted by regularly testing and validating AI/ML models using real-world data and implementing robustness techniques such as adversarial training to defend against adversarial attacks while continuously monitoring model performance and updating the models as necessary.

- **Regulatory Compliance Risks:** The use of AI and ML in banking may raise concerns about compliance with financial regulations and consumer protection laws.
    - **Mitigation:** Working closely with regulators, establishing internal governance and compliance frameworks, and ensuring transparency in AI decision-making processes would go a long way in managing these risks.

OPEN BANKING

Open banking drives innovation in the banking industry, allowing customers to securely share financial data with other institutions. Use cases include:

- **Personal Finance Management:** Accessing all financial accounts in one place through open banking enables better financial management.
- **Improved Loan and Credit Assessment:** Lenders can access real-time financial data for accurate credit risk assessments.
- **Account Aggregation:** Customers can consolidate accounts from multiple banks into a single interface, simplifying financial tracking.
- **Payment Initiation Services:** Third-party providers can initiate payments on behalf of customers, enabling faster and more convenient payment options.
- **Enhanced Financial Services:** Fintech companies develop innovative products, leveraging open banking data.

Risks and Mitigation Measures:

- **Cybersecurity Risks:** Open APIs can become targets for cyber-attacks, leading to unauthorized access, data manipulation, and service disruptions.
    - **Mitigation:** Utilization of firewalls, intrusion detection systems, conducting regular penetration testing, and developing an incident response plan would assist in mitigating these exposures.

- **Data Access and Consent Risks:** Data access and consent risks in open banking pertain to the handling of customer financial data and the permissions granted by customers to share their data with third-party financial service providers. These risks encompass unauthorized data access, inadequate consent mechanisms, and the potential for consent fraud and social engineering, which may lead to privacy breaches and unauthorized access to sensitive information. Moreover, data aggregation in open banking platforms poses additional risks, as it increases data exposure and could result in privacy violations. Collaboration with third-party providers also introduces the risk of data misuse, potentially eroding customer trust. Managing consent preferences and complexity further challenge data access and consent controls.
    - **Mitigation**: Banks should ensure explicit and informed customer consent before accessing their financial data through open banking APIs and implement secure and standardized consent management mechanisms to give customers control over data access. Regularly reviewing and updating consent agreements based on customer preferences and changing regulations is also imperative.

HYPER-PERSONALIZATION IN BANKING

Hyper-personalization requires a comprehensive view of customers, assimilating information from varied sources to offer tailored experiences. Use cases include:

- **Personalized Product Recommendations:** Offering personalized product recommendations based on financial goals and risk preferences.
- **Dynamic Pricing:** Tailoring pricing based on individual customer behaviours, transaction histories, and preferences.
- **Customized User Interfaces:** Prioritizing relevant information and services based on customer preferences.
- **Contextual Offers:** Sending real-time, context-aware offers and promotions based on current financial situations and spending patterns.
- **Personalized Financial Insights:** Delivering customized financial insights and recommendations to customers.

Risks and Mitigation Measures:

- **Over-Reliance on Algorithms:** Hyper-personalization relies on sophisticated algorithms and AI systems. An over-reliance on these algorithms without proper human oversight can lead to incorrect decisions, customer dissatisfaction, and financial losses.
    - **Mitigation:** To avert the risks, the bank should maintain a human-in-the-loop approach, regularly audit and update algorithms.

BLOCKCHAIN IN BANKING

Blockchain can significantly transform the banking sector with various applications:

- **Cross-Border Payments:** Facilitating faster and cost-effective cross-border payments by eliminating intermediaries.
- **Trade Finance:** Streamlining trade finance processes with a transparent and secure platform for verifying trade documents.
- **KYC and AML Compliance:** Enhancing KYC and AML processes with secure and immutable customer identity records.
- **Supply Chain Management:** Improving supply chain transparency and traceability by recording goods' provenance.
- **Digital Identity Verification:** Offering decentralized and tamper-proof digital identity verification for online transactions.

Risks and Mitigation Measures:

- **Smart Contract Risks:** Smart contracts, which are self-executing code on the blockchain, can have coding errors or vulnerabilities, leading to financial losses and disruptions in business operations.
    - **Mitigation:** Conducting thorough code audits, implementing multi-signature authorization for critical smart contract operations is critical.
- **Regulatory Compliance Risks:** The adoption of blockchain technology may raise concerns about compliance with existing financial regulations and data protection laws.
    - **Mitigation:** One needs to work closely with regulators and develop internal governance frameworks.

IMMERSIVE TECHNOLOGIES AND METAVERSE

With the metaverse gaining traction and popularity among users, it’s only a matter of time before banks start leveraging this technology to enhance its services. Immersive technologies like the metaverse can enhance banking services in various ways:

- **Virtual Branches:** Creating virtual branches for customer interactions and personalized financial services.
- **Financial Education:** Offering engaging and interactive financial education programs.
- **Virtual Tours and Property Visualization:** Providing virtual property tours and investment opportunities.
- **Virtual Meetings and Events:** Hosting virtual meetings, seminars, and events.
- **DeFi Integration:** Exploring integration with DeFi platforms for innovative financial products.

Risks and Mitigation Measures:

- **Unforeseen Risks:** Immersive technologies and metaverse platforms can become targets for identity fraud if not equipped with robust user authentication measures.
    - **Mitigation:** Immersive technologies and metaverse platforms are potential targets for cyberattacks, leading to unauthorized access, data breaches, and service disruptions.

ROBOTIC PROCESS AUTOMATION (RPA) IN BANKING

RPA streamlines back-office tasks, improving efficiency and accuracy. Use cases include:

- **Customer Onboarding:** Automating document verification and compliance procedures for faster onboarding.
- **Loan Processing:** Automating loan application processing and credit scoring.
- **Account Reconciliation:** Automating account reconciliation processes.
- **Fraud Detection:** Real-time analysis for detecting and flagging suspicious activities.
- **Customer Support**: AI-powered chatbots for 24/7 customer support.

Risks and Mitigation Measures:

- **Integration Complexity Risks:** Integrating various banking systems and third-party tools for process automation can lead to integration complexities and potential points of failure.
    - **Mitigation:** In order to avert these, one needs to conduct thorough testing, implement error handling, and monitoring mechanisms.
- **Dependency on Technology Risks:** Overreliance on technology for banking processes may lead to disruptions in case of system failures, cyberattacks, or technical glitches.
    - **Mitigation:** Establishing robust business continuity plans and maintaining redundancies and backups helps in its management.

CLOUD BANKING

Cloud banking offers cost efficiency, scalability, innovation, and accessibility. Use cases include:

- **Cost Efficiency:** Reducing infrastructure and maintenance costs.
- **Scalability:** Easily scaling resources based on demand.
- **Innovation:** Facilitating faster development of new services and products.
- **Accessibility:** Enabling customers to access accounts and perform transactions from anywhere.

Risks and Mitigation Measures:

- **Service Availability Risks**: Relying on cloud service providers for critical banking operations can lead to service disruptions if the provider experiences outages or technical issues.
    - **Mitigation**: Establishing service level agreements and maintaining redundancies and backups would help reduce such exposures.
- **Compliance Risks:** Storing customer data on cloud servers may raise concerns about compliance with data protection laws and financial regulations.
    - **Mitigation:** Choosing cloud providers that comply with relevant data protection regulations and industry certifications alongwith developing internal governance frameworks to monitor cloud provider compliance and data handling practices is essential.

QUANTUM COMPUTING

As the development of quantum computing progresses, it is crucial for banks to proactively address digital risks through the adoption of quantum-safe technologies and security measures. By staying ahead of potential threats and embracing quantum-enhanced applications, banks can capitalize on the benefits of this transformative technology while maintaining the security and trust of their customers and financial systems. Some of its uses in banking are:

- **Enhanced Portfolio Optimization:** Quantum computing can significantly speed up portfolio optimization algorithms, allowing banks to efficiently allocate assets and manage risk more effectively, leading to improved investment strategies and higher returns.

- **Fraud Detection and Prevention:** Quantum computing's processing capabilities can help banks analyze vast amounts of transaction data in real-time, enabling quicker identification of fraudulent activities and enhancing fraud prevention measures.
- **Credit Risk Assessment:** Quantum computing can accelerate credit risk modelling and assessment, leading to more accurate credit scoring and enabling banks to make better-informed lending decisions.
- **Quantum Encryption for Secure Communications:** Banks can leverage quantum encryption techniques to establish secure communication channels between branches and customers, protecting sensitive information from quantum hacking attempts.
- **Algorithmic Trading:** Quantum computing's ability to perform complex calculations swiftly can be employed in algorithmic trading strategies, allowing banks to optimize trading performance and respond rapidly to market changes.

The risks and mitigation measures are:

- **Data Security Risk:** Quantum computing's immense processing power poses a threat to traditional encryption algorithms used to protect sensitive data in the banking sector. Quantum computers can potentially break current encryption methods, making customer data, transactions, and other confidential information vulnerable to unauthorized access and cyberattacks.
  - **Mitigation:** Banks should implement a roadmap for updating cryptographic protocols and systems, ensuring they are quantum-resistant, and conduct thorough security audits to identify and address potential vulnerabilities.
- **Disruption of Digital Signatures and Authentication:** Quantum computing can compromise the security of digital signatures and authentication mechanisms that underpin secure transactions and identity verification. This could lead to unauthorized access, fraudulent activities, and identity theft.
  - **Mitigation:** Banks may enhance security by combining multiple authentication factors, such as biometrics, one-time passwords, and hardware tokens, to strengthen identity verification and reduce the risk of unauthorized access.

In addition to the above mentioned risks, there are risks which are commonly applicable to all these new and emerging technologies. These risks are namely:

- **Data Security and Privacy Risks:** New technologies such as AI, Blockchain etc. in banking requires extensive data processing and storage, making banks more susceptible to data breaches and privacy violations. Some banking involves sharing customer financial data with third-party providers through APIs, posing potential risks of data breaches and privacy violations if the data is not adequately protected. Some also involve collecting and processing vast amounts of customer data for personalized experiences, creating potential data security and privacy vulnerabilities if not adequately protected.
  - **Mitigation**: In order to mitigate these, one should implement robust data encryption and access controls, comply with data protection regulations, and establish strong data governance policies.
- **Identity Fraud and Authentication Risks:** The sharing of customer data across multiple platforms increases the risk of identity theft and fraudulent transactions if proper authentication measures are not in place.
  - **Mitigation:** In order to manage these risks one should implement multi-factor authentication and monitor customer activity for unusual behaviour. Educating the customers on the best practices for securing their personal information is also critical. Implement secure and multi-factor authentication methods to verify user identities within immersive environments. Continuously monitor user activities for suspicious behaviour and take immediate action against potential fraudulent activities. Educate customers about best practices for protecting their personal information.

The findings of this research have significant implications for enhancement of digital risk management practices in the bank. A proactive and comprehensive approach is necessary to mitigate digital risks effectively. The bank should conduct regular risk assessments, update its incident response plans, and prioritize data protection measures on par with the evolving technological landscape.

Moreover, staff should be adequately trained in the management and awareness of new technologies in order to promote a culture of digital risk awareness. Such education may include training sessions, simulated phishing exercises, and continuous reinforcement of security best practices. By empowering its staff and other stakeholders to recognize and respond to potential risks, the bank can significantly reduce the likelihood of falling prey to digital attacks and incidents.

8. LIMITATIONS

Emerging technologies often lack extensive historical data, making it challenging to conduct longitudinal studies or establish robust baselines. The limited data restricted the depth of analysis of trends and behaviour. Furthermore, due to the fast paced nature of technology, some of the technologies mentioned may become outdated or new technologies might emerge at the time of publication of this research. Also, due to the novelty of these technologies, expertise in these fields are limited and thus a considerable level of difficulty was faced in comprehending the uses and capabilities of these technologies.

9. CONCLUSION

Embracing technological advancements in the banking sector offers tremendous opportunities, but it also comes with potential risks. By implementing robust mitigation measures, banks can confidently leverage AI and ML, open banking, hyper-personalization, blockchain, immersive experiences, RPA, and cloud banking to enhance services, streamline operations, and deliver outstanding customer experiences while safeguarding data and ensuring compliance with regulations. Proactively addressing these digital risks will pave the way for a secure and prosperous future for the banking industry. Looking ahead, emerging technologies like artificial intelligence and machine learning hold promise in enhancing digital risk management. These technologies can assist in real-time threat detection, anomaly detection, and automated incident response. However, careful consideration must be given to the ethical implications and potential biases associated with these technologies. Effective digital risk management is crucial in today's rapidly evolving digital landscape. This research has explored the strategies employed by organizations to manage digital risk, highlighting the importance of risk assessment, incident response planning, data protection measures, and employee awareness programs. It has also identified the challenges organizations face and suggested recommendations for improving digital risk management practices. By implementing comprehensive strategies, staying informed about emerging threats, and fostering a culture of cybersecurity awareness, the bank can enhance its resilience to digital risks and protect their valuable assets and data.

10. REFERENCES

1. How will artificial intelligence and Industry 4.0 emerging technologies transform operations management? (2022) by Sunil Mithas, Zhi-Long Chen, Terence J.V. Saldanha and Alysson De Oliveira Silveira
2. Is digital transformation threatened? A systematic literature review of the factors influencing firms' digital transformation and internationalization (2023) by María M. Feliciano-Cestero, Nisreen Ameen, Masaaki Kotabe, Justin Paul and Mario Signoret
3. A survey on security in internet of things with a focus on the impact of emerging technologies (2022) by Phillip Williams, Indira Kaylan Dutta, Hisham Daoud and Magdy Bayoumi
4. Digital Risk Management in Banking(2019) by RSA
5. Managing Risks to get fit for a Better Future(2023) by Deloitte
6. Exploring research trends of emerging technologies in Health Metaverse: a bibliometric analysis(2022) by Donghua Chen and Runtong Zhang
7. A general framework of digitization risks in international business(2022) by Yadong Luo
8. Analysis of the adoption of emergent technologies for risk management in the era of digital manufacturing(2023) by Oscar Rodríguez-Espíndola, Soumyadeb Chowdhury, Prasanta Kumar Dey, Pavel Albores and Ali Emrouznejad