International Journal of Management Information Systems and Data Science ,2024;1(2):26-37

ADVANCING DATA SECURITY IN GLOBAL BANKING: INNOVATIVE BIG DATA MANAGEMENT TECHNIQUES

Mahmudul Hasan[1], Md Mostafizur Rahman[2], Md Shakawat Hossain[3], Md Abdul Ahad Maraj[4]

[1] Graduate Researcher, Management Information System, College of Business, Lamar University, Beaumont, Texas, US

[2] Graduate Researcher, Management Information System, College of Business, Lamar University, Beaumont, Texas, US

[3] Graduate Researcher, Management Information System, College of Business, Lamar University, Beaumont, Texas, US

[4]Graduate Researcher, Management Information Systems, College of Business, Lamar University, Beaumont, Texas, USA.

Keywords

Big Data
Data Security
Banking Industry
Regulatory Complianc
Global Banks.

ABSTRACT

In the context of the rapidly evolving digital landscape, the banking sector faces unprecedented challenges in data security due to the massive volumes of sensitive information they manage. This paper examines the implementation and efficacy of innovative big data management techniques within global banking institutions to enhance data security. It discusses the integration of predictive analytics, the impact of regulatory changes, and the adoption of emerging technologies like blockchain and advanced encryption, which collectively redefine data security strategies. The study utilises a qualitative case study approach focusing on three central banks—JPMorgan Chase & Co., HSBC Holdings plc, and the Industrial and Commercial Bank of China—highlighting how each bank utilises big data techniques to address specific security challenges, comply with regulations, and enhance customer trust. The findings underscore the crucial role of innovative data management strategies in mitigating risks and safeguarding data against cyber threats, suggesting that these technologies fulfil security needs and offer competitive advantages in customer trust and regulatory compliance. The paper concludes with strategic recommendations for banks to enhance their data security measures and suggests directions for future research in data security within the banking industry.

1 Heading

The rise of the digital economy has significantly increased the volume of sensitive data managed by banks, encompassing everything from personal identification details to comprehensive financial records (Bholat, 2015). As custodians of critical information vital to individual security and the broader stability of the financial sector, banks have become attractive targets for cybercriminals (Alzoubi, Alshurideh, et al., 2022; Alzoubi, Ghazal, et al.,

2022). These criminals continually refine their methods, increasing the sophistication of their attacks. The stakes are high, as the potential consequences of a data breach within a financial institution extend well beyond the immediate financial losses (Al Kurdi et al., 2020; Lee & Chen, 2022). Such incidents can also lead to long-lasting reputational damage and incur heavy regulatory penalties. The complex and evolving nature of these threats underscores the critical need for banks to adopt robust and innovative data security measures to safeguard this sensitive information (Hoffmann & Birnbrich, 2012).

The sensitivity and scale of data bank management necessitate implementing highly secure data management practices. Big data technologies offer significant potential to innovate and enhance these security measures within the banking sector (Lee & Chen, 2022). By facilitating the management and analysis of vast, complex datasets, big data applications provide opportunities to bolster the security posture of financial institutions. This is increasingly important as banks intensify their focus on cybersecurity, aiming to protect assets and maintain global financial stability (Al Kurdi et al., 2020). The use of advanced big data tools in this context helps preempt and mitigate risks and supports the broader objectives of financial security and customer trust in the digital era. Exploring big data management techniques to enhance bank data security is a subject of considerable interest and potential (Bholat, 2015). Understanding how these technologies can be effectively leveraged is vital for safeguarding sensitive information and addressing the persistent threat of cyberattacks. The focus on advanced data management practices within the banking sector is essential for strengthening security mechanisms, aligning with broader objectives such as enhancing customer trust—a critical element in maintaining the integrity and reliability of the financial system (Bholat, 2015; Fuller, 2015). This alignment underscores the importance of continuous improvements in data security protocols to cope with the complexities of modern cyber threats.

2 Literature Review

The literature on this topic is extensive and multifaceted, addressing various aspects of significant data adoption, from the technical challenges of integration to the strategic implications for business operations. This literature review aims to synthesise key findings from various sources to provide a comprehensive overview of the current state of big data in banking. It explores the technical challenges associated with implementing these technologies, the regulatory landscape that governs their use, and the financial considerations that impact their adoption. Additionally, the review examines the transformative potential of big data in enhancing operational efficiency, improving customer experiences, and facilitating innovation in financial services. Drawing on recent studies, industry reports, and theoretical perspectives, this section

3 Method Big Data in Banking

Integrating big data analytics into banking operations offers transformative possibilities for improving various aspects of the sector (Chen et al., 2012; Chui et al., 2019). Primarily, the application of big data significantly enhances fraud detection capabilities. By utilising machine learning algorithms in conjunction with the analysis of extensive datasets, banks can identify patterns and anomalies that may signify fraudulent activities, thereby bolstering their security measures (Varian, 2014)—furthermore, big data analytics aids in refining risk modelling processes. Financial institutions can better predict and assess potential risks, such as loan defaults and market volatility, with more precise and comprehensive data analysis. This capability enables banks to develop more effective risk mitigation strategies for maintaining financial stability (Chen et al., 2012; Sun et al., 2019). Additionally, big data plays a pivotal role in personalising customer experiences in the banking industry. Banks can customise their services, offers, and communications through detailed customer data analysis to meet their clients' unique preferences and needs. This tailored approach enhances customer engagement and significantly increases satisfaction levels. As banks leverage big data to fine-tune their operations, the benefits extend beyond improved security and risk management to fostering deeper client relationships and loyalty (Mahi, 2024). These advancements underscore the critical role of big data analytics in driving innovation and efficiency within the banking sector.

The implementation of big data within the banking sector, while offering substantial benefits, also introduces significant security challenges that must be addressed to safeguard sensitive information effectively. One primary concern is the expanded attack surface that comes with the vast volumes of data characteristic of extensive data systems, providing cybercriminals with more potential entry points (Hanaysha et al., 2021). Consequently, banks must implement increasingly robust security measures to protect these numerous vulnerabilities. Additionally, the inherent nature of big data involves the distributed storage and processing of data across multiple systems, complicating the security landscape. Ensuring comprehensive security across all these distributed components presents a complex challenge that requires sophisticated and coordinated security strategies (Kahn et al., 2002).

Figure 1:Big Data Challenges in Banking

The banking industry benefits from a higher standard of data quality compared to many other sectors. This is attributed to customer onboarding requirements requiring accurate and detailed personal information. Banks meticulously track customer transactions, credit histories, and behaviours across online and traditional channels. Accordingly, a primary challenge the banking industry faces is the high dimensionality of data, exceeding the volume of concerns prevalent in domains like e-commerce (Lee et al., 2022). Customer clustering represents a widely used analytic method within the banking sector (Ghazal et al., 2021). However, high dimensionality complicates analysis and interpretation (Rahaman & Bari, 2024). Even with large sample sizes, customer clustering can lead to challenges such as disproportionately dense clusters, hindering meaningful insights (Hanaysha et al., 2021). While various clustering methods for high-dimensional data exist (Ghazal et al., 2021), the results can still lack clarity of interpretation for end-users. Without easily understandable results, it becomes difficult for data scientists to promote the value of their models and optimise their impact. Accurate evaluation of big data analytics within banking presents unique difficulties. While A/B testing and baseline comparisons are standard methods, defining appropriate baselines amidst ongoing operations can be complex. Commonly used performance indicators include revenue generation and response rates (Bholat, 2015). It is important to note that a high response rate does not guarantee a proportionally high monetary return.

Moreover, the integrity and quality of the data in extensive data systems are crucial. Data poisoning, where data is corrupted or manipulated, poses a significant risk as it can lead to inaccurate insights and potentially flawed decision-making processes (Rasouli, 2019). Banks are thus compelled to establish rigorous protocols to verify the quality of data inputs and ensure the reliability of the analytic outputs. This includes continuous monitoring and validation of data to prevent and mitigate the risks associated with data corruption or manipulation, ensuring that decision-making is based on accurate and reliable information (Sadok et al., 2022). The complexities these factors introduce underscore the need for advanced security measures and quality assurance in managing big data within the banking industry.

4 Big Data Security Techniques

Zero-trust architecture (ZTA) signifies a significant evolution in the approach to banking security. Unlike traditional perimeter-based security models (AlHamad et al., 2012), ZTA hinges upon the core concept of "never trust, always verify." This approach mandates the continuous authentication and authorisation of all users and actions seeking to interact with data. ZTA strategies limit access according to the principles of least privilege and need-to-know, effectively minimising the risk of unauthorised access and the spread of internal threats. ZTA implementation involves several vital components (Al Shebli et al., 2021; Alshamsi et al., 2020). Robust identity and access management (IAM) systems ensure that every user and device seeking access undergoes rigorous authentication and verification protocols. Micro-segmentation techniques divide the network into smaller, isolated zones, minimising the scope of potential breaches by restricting lateral movement (Ali et al., 2022; Alshurideh et al., 2019). Comprehensive monitoring and logging mechanisms provide continuous visibility into network activity, allowing for the swift detection of anomalies. By adopting a zero-trust approach, banks enhance the protection of their sensitive data. This proactive security framework limits potential attack surfaces, reduces the likelihood of successful breaches, and enhances an organisation's overall security posture (Zhang et al., 2019). As cyber threats evolve, zero-trust models will likely become increasingly prevalent within the banking industry.

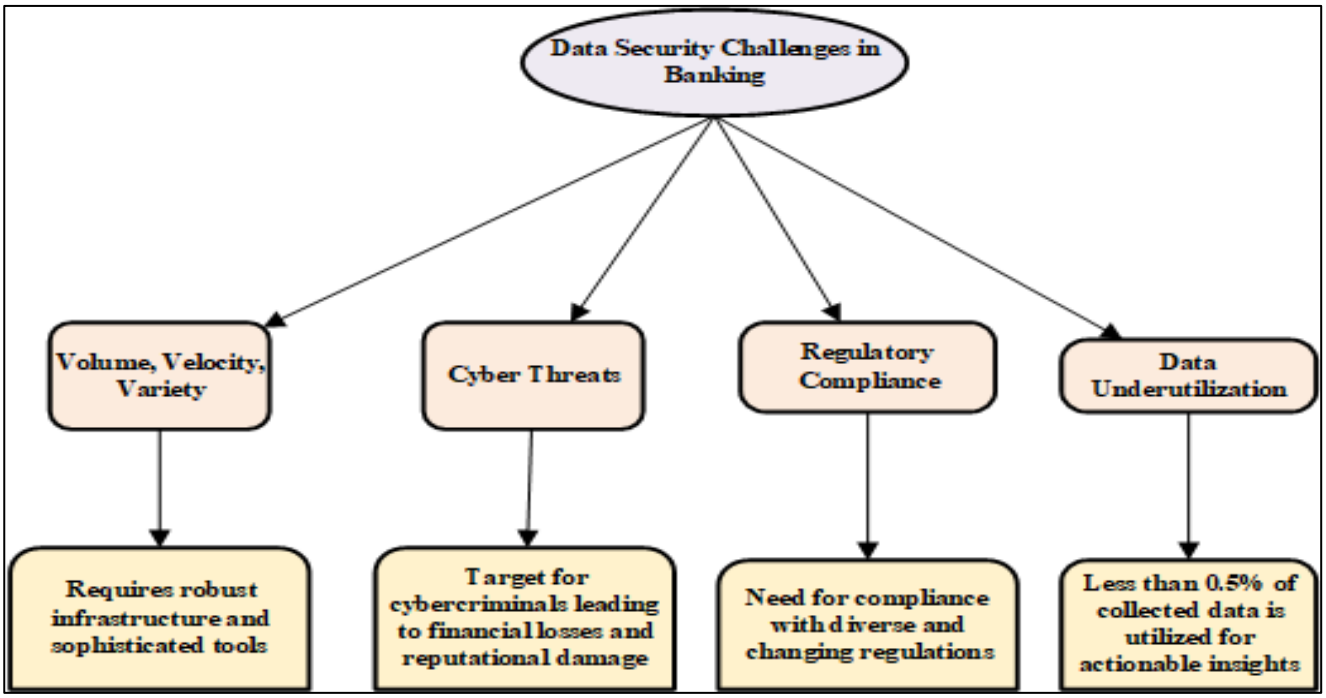
Advanced encryption techniques offer a heightened level of security for data within the banking sector. Homomorphic encryption stands out for safeguarding data confidentiality while computations are performed (Alshamsi et al., 2020; Chui et al., 2019). This eliminates the need to temporarily decrypt data for analysis, thereby minimising windows of vulnerability. Secure multi-party computation (SMC) enables collaborative analytics scenarios where multiple entities can derive insights from combined datasets without compromising the privacy of their respective data sources (Chui et al., 2019; Gandomi & Haider, 2015). Differential privacy provides a rigorous framework for balancing the utility of data analysis with protecting individual privacy. This technique carefully introduces calibrated noise into datasets, obscuring individual records while preserving aggregate statistical properties. Banks can leverage differential privacy to generate insights that are compliant with privacy regulations, maintaining customer trust while driving informed decision-making. The strategic adoption of these advanced encryption techniques significantly bolsters banks' security posture (AlHamad et al., 2012; Zhang et al., 2019). By safeguarding the privacy and integrity of financial records during various stages of use - whether in transit, at rest, or during collaborative processing - these techniques proactively mitigate the risk of unauthorised data access and breaches. Their implementation demonstrates a commitment to robust data security practices, aligning with the industry's strict standards in handling sensitive information.

5 Data Security Challenges in Banking

The banking sector has experienced significant transformation due to the advent of intelligent data-driven technology systems. An enormous amount of data is now captured and stored, characterised by unprecedented volume, velocity, and variety. This surge in data, coupled with the rapid development of new technologies such as artificial intelligence (AI), the Internet of Things (IoT), big data analytics (BDA), cloud computing, and blockchain, has profoundly impacted business strategies and management practices across the financial landscape (Chui et al., 2019). Historically, the importance of data innovation was often overlooked in business operations; however, its value is now widely recognised, and most companies globally have begun to capitalise on the opportunities presented by big data (Barker et al., 2008). Despite the substantial investment in data capture and storage, it is reported that less than 0.5% of the collected data is analysed or utilized (Hasan et al., 2012; O'Brien, 2010). This underutilisation highlights a critical gap in the ability of financial institutions to transform data into actionable insights and knowledge that can drive management decisions and generate profit (Chen et al., 2012; Hasan et al., 2020). As a result, banks and other financial entities are increasingly focused on developing

strategies to manage and effectively use this vast amount of information to enhance their operational efficiencies and competitive advantage. This shift underscores a growing recognition of the need to gather, intelligently analyse and apply big data to sustain and enhance business operations in the increasingly digital and data-driven financial sector (Dattaram & Madhusudanan, 2016).

Figure 2: Data Security Challenges in Banking



Data innovation, mainly through big data, has become a pivotal concept in the evolution of the banking and financial services sector. This revolution is enhancing the ability of banks to understand and cater to customer preferences, ultimately improving service quality, increasing profits, and enhancing customer satisfaction (El Khatib et al., 2022). Large volumes of customer data enable banking organisations to tailor their services more effectively, responding to individual customer needs more precisely. Furthermore, the rapid advancement of data analytics technology has introduced a range of new services in the banking sector, significantly enhancing the ability to specialise and personalise product offerings (Bonsón & Flores, 2011). As the competitive landscape in the banking industry intensifies, understanding customer behaviour through data analysis becomes crucial. Insights derived from big data help banks improve existing customer relationships and attract similar new customers, thereby expanding market share (Alzoubi & Ahmed, 2019). Moreover, significant data innovation is broadening financial institutions' business scope and service offerings, offering them new avenues for growth and development. Despite these advantages, the sector faces challenges related to the vast diversity and volume of data, which complicates decision-making processes. Banks must collect and integrate data and transform it into strategic assets that enhance customer satisfaction and overall company performance (Tariq et al., 2022). Effective data use requires deep mining to uncover valuable insights that can be leveraged to offer better financial products and services. Challenges include processing large, multi-source datasets quickly and efficiently, managing fragmented data from various financial technologies, and mitigating risks associated with rapid response demands. The overarching goal for banks is to harness data analytics and mining to unlock hidden information that can drive more significant economic benefits and improve operational efficiency in a highly competitive industry (Muheidat et al., 2022).

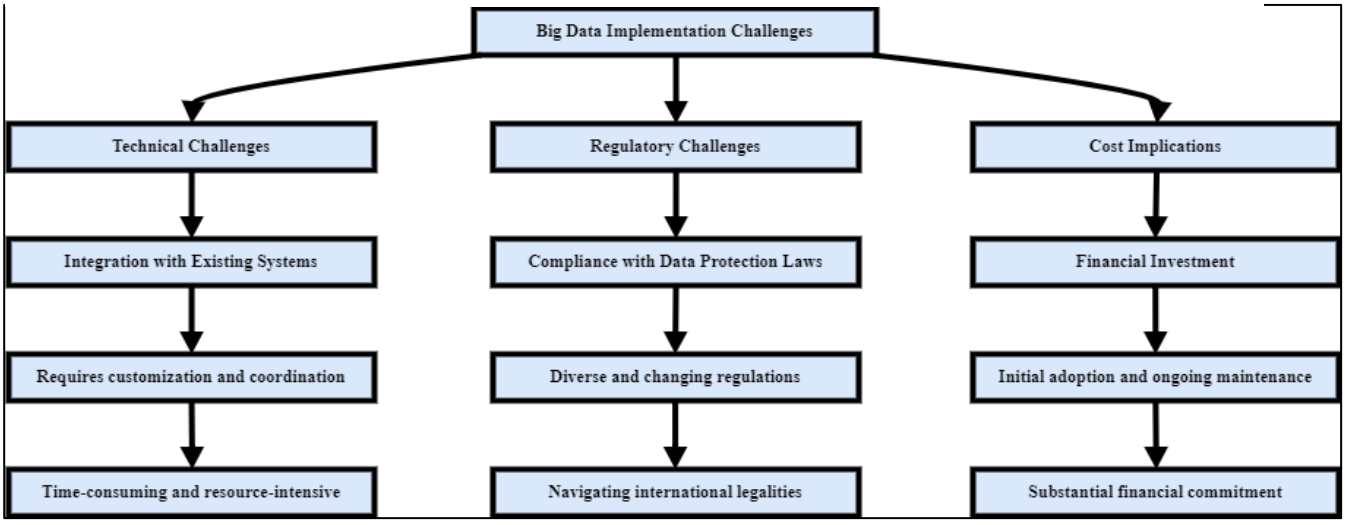
In the banking sector, data security challenges are prevalent and multifaceted, reflecting the sensitivity and vastness of the data handled. Banks face significant

threats from cybercriminals who target the wealth of personal and financial information stored within their systems (Al Kurdi et al., 2020; Alshurideh, 2022). Case studies of significant data breaches in the banking industry illustrate severe consequences, including substantial financial losses, regulatory penalties, and lasting reputational damage, affecting the institutions and their customers (Wei et al., 2012). The economic impact of these breaches can be profound, eroding customer trust and potentially leading to a loss of business. At the same time, the reputational damage can alter consumer perceptions and confidence for years. Within banking, big data encompasses collecting, processing, and analysing vast amounts of digital information to enhance decision-making processes. Banks utilise big data for various purposes, including gaining customer insights through behaviour analysis, enhancing risk management protocols, and detecting fraud more effectively. These applications demonstrate big data's critical role in improving service delivery and operational efficiency (Muheidat et al., 2022). However, managing large datasets is challenging— data volume, velocity, and variety present significant hurdles. The sheer amount of data generated daily requires robust infrastructure for effective management. In contrast, the speed at which data flows necessitates real-time processing capabilities, and the diversity of data type s demands sophisticated tools for analysis and interpretation (Alzoubi et al., 2020)

6 Challenges in Implementing Big Data Techniques

Implementing big data techniques in the banking sector presents several challenges that institutions must navigate to harness the full potential of this technology (Alzoubi et al., 2020; Tariq et al., 2022). One of the primary technical challenges involves the complexity of integrating new data technologies with existing banking systems. This integration often requires substantial customisation and coordination to ensure that new and old systems work seamlessly together, a process that can be both time-consuming and resource-intensive (Al-Khayyal et al., 2020; Kaisler et al., 2013). Regulatory challenges pose significant hurdles, as banks must comply with a complex web of global and regional data protection laws. These regulations are designed to protect consumer data and ensure privacy, but adhering to them can be formidable given their diversity and the rapid pace of legislative changes. Each jurisdiction may have its rules, and banks operating internationally must be adept at navigating them to avoid legal penalties and safeguard customer trust (Hoffmann & Birnbrich, 2012; Sun et al., 2019). Moreover, the cost implications of adopting big data technologies cannot be underestimated. Significant investment is often required for the initial adoption of these technologies and ongoing maintenance and updates. Banks must allocate considerable financial resources to ensure that their data management systems are state-of-the-art and capable of handling the vast amounts of data generated daily. This investment is crucial for

Figure 3: Big Data Implementation Challenges



maintaining competitive advantage and operational efficiency but represents a substantial financial commitment (Alshurideh et al., 2022; Madakam et al., 2019). These challenges underscore the complexities of leveraging big data within the banking industry, necessitating a strategic approach to overcome technical, regulatory, and financial barriers.

7 Method

This study employed a qualitative, multiple-case study design to investigate the implementation and challenges of big data techniques within the global banking sector. Three internationally recognised institutions were selected: JPMorgan Chase & Co. (USA), HSBC Holdings plc (UK), and Industrial and Commercial Bank of China (China). This strategic selection enabled cross-case comparative analysis across distinct regulatory environments, providing insights into variations in big data implementation strategies. A multi-method data collection approach was used, including semi-structured interviews with key stakeholders (e.g., IT executives, data scientists, compliance officers), analysis of internal reports, project documentation, public disclosures, and limited observational techniques. This comprehensive methodological framework aimed to generate a nuanced understanding of the complexities and evolving practices surrounding extensive data adoption within the banking industry.

8 Findings

The motivations driving significant data adoption varied significantly across the three studied banks, each aligning with their strategic objectives and operational needs. JPMorgan Chase & Co. heavily leveraged big data for customer personalisation and enhanced risk modelling. This focus was primarily driven by the potential to optimise revenue growth through tailored customer service offerings and more accurate risk assessments. On the other hand, HSBC Holdings plc concentrated on significant data initiatives that supported regulatory compliance efforts. This strategic priority aimed to minimise the risk of regulatory fines and sanctions, a significant concern for global banks operating under stringent regulatory environments like GDPR. In contrast, the Industrial and Commercial Bank of China prioritised fraud prevention as the primary driver of its significant data investments, seeking to protect assets and maintain customer trust in a market sensitive to the repercussions of financial fraud. All three banks faced common hurdles regarding data security challenges, each with unique complications based on their operational context. A widespread issue was the shortage of specialised talent capable of managing data privacy and conducting secure analytics, which is critical in the era of increasing cyber threats. Additionally, modernising legacy systems to manage the volume and complexity of big data incurred substantial costs, often exceeding initial project budgets. HSBC Holdings plc, for example, dealt with specific challenges related to GDPR compliance, which imposed strict data retention policies that temporarily hindered the availability of historical data essential for some of their analytics models. Meanwhile, regulatory conditions in China posed distinct challenges for the Industrial and Commercial Bank of China, influencing its data collection and analysis practices and requiring the development of alternative analytical methods to comply with national regulations.

The case studies also highlighted the critical role of collaboration among various departments within the banks to ensure the successful implementation of big data projects. This was particularly evident in forming interdisciplinary governance committees, which are pivotal in effective decision-making and risk management across all three institutions. At JPMorgan Chase & Co., a robust data governance framework was essential for ensuring compliance and data security and enhancing data quality and accuracy. This improvement in data management significantly boosted the effectiveness of the bank's targeted marketing initiatives and overall customer engagement strategies. Through these collaborative efforts, each bank navigated the complexities of significant data adoption more effectively, aligning technology innovations with their strategic business goals.

Figure 4: Summary of the findings

Bank	Motivation for Big Data Adoption	Challenges Faced	Strategies for Success
JPMorgan Chase & Co.	Customer personalization and enhanced risk modeling to optimize revenue growth	• Shortage of specialized talent • Modernizing legacy systems	• Formation of interdisciplinary governance committees • Robust data governance framework
HSBC Holdings plc	Regulatory compliance to minimize the risk of fines and sanctions	• GDPR compliance challenges affecting data availability • Shortage of specialized talent • Modernizing legacy systems •	• Formation of interdisciplinary governance committees • Adaptation to GDPR requirements
Industrial and Commercial Bank of China	Fraud prevention to protect assets and maintain customer trust	• Regulatory conditions in China requiring alternative analytical methods • Shortage of specialized talent • Modernizing legacy systems	• Formation of interdisciplinary governance committees • Development of alternative analytical methods to comply with national regulations

9 Discussion

The discussion surrounding adopting big data in banking reveals a nuanced landscape of motivations and challenges, with notable similarities and differences compared to findings from similar studies. JPMorgan Chase & Co.'s emphasis on using big data for customer personalisation and risk modelling aligns with broader financial services industry trends. For instance, a study by Al Kurdi et al. (2020) highlighted that many North American banks prioritise big data to capitalise on the potential for revenue growth and operational optimisation. This approach mirrors JPMorgan Chase & Co.'s strategy, suggesting a typical industry trajectory towards leveraging big data to enhance profitability and customer service. However, unlike some European banks, which, as noted by Al-Khayyal et al. (2020), tend to focus more heavily on risk compliance due to the region's strict regulatory environment, JPMorgan Chase & Co. demonstrates a more balanced approach between growth and compliance (Skyrius et al., 2016).

HSBC Holdings plc's focus on regulatory compliance through significant data initiatives reflects the growing global emphasis on meeting stringent legal standards, particularly in regions affected by regulations like GDPR. This focus is crucial, as highlighted by Kaisler et al. (2013), who point out that failure to comply with such regulations can result in severe penalties and damage to reputation. However, HSBC's approach also reveals the practical difficulties of adapting big data strategies within the constraints of regulatory frameworks, a challenge less pronounced in regions with more lenient data laws. The experience of HSBC offers a critical lesson on the importance of flexible data strategies that can adjust to varying regulatory demands. Moreover, the Industrial and Commercial Bank of China's prioritisation of fraud prevention through big data indicates the heightened security needs within the Chinese banking sector, where digital payment systems are extensively used. This focus

is well-aligned with findings from Hoffmann and Birnbrich (2012), who noted that Asian banks increasingly leverage big data to combat sophisticated cyber threats. The emphasis on fraud prevention in this region contrasts with Western banks, which, while also concerned with security, often balance this with innovations aimed at customer experience and service diversification. The differing priorities underscore regional variations in significant data adoption, influenced by cultural, economic, and regulatory factors.

In addition, the shared emphasis on cross-departmental collaboration and robust governance frameworks across the three banks echoes broader industry findings regarding the critical role of internal organisational structures in successful extensive data implementation. Research by Fayyad et al. (2001)supports this observation, highlighting that effective big data strategies are often underpinned by solid leadership and integrated teamwork across IT, data science, and compliance departments. These studies affirm that while the specific applications and challenges of big data may vary by institution and region, the fundamental need for comprehensive governance and collaborative frameworks remains consistent across the banking industry (Mahi, 2024). This convergence suggests that regardless of the particular focus—compliance, customer service, or security—the success of significant data initiatives often hinges on how well an organisation can effectively align its internal structures and cultures to leverage these powerful technologies.

10 Conclusion

In the era of big data, the importance of robust data security for banks cannot be overstated, as it is crucial for protecting sensitive information and maintaining customer trust. Predictive analytics significantly enhances data security by enabling banks to anticipate and mitigate potential threats proactively. As regulations evolve, banks must adapt their data management strategies to comply with new standards while ensuring adequate security. Emerging technologies, such as blockchain and advanced encryption methods, continue redefining the data security landscape in banking, offering new tools to protect against cyber threats. A study recap highlights the effectiveness of innovative data management techniques, demonstrating their potential to mitigate risks significantly. Banks are recommended to embrace these technologies as security measures and competitive advantages that can enhance customer trust and ensure compliance with regulatory requirements. Furthermore, there is a pressing need for continuous research to explore new technologies and methodologies that could further advance data security in the banking sector, ensuring that financial institutions remain resilient against the ever-evolving landscape of cyber threats.

References

Al-Khayyal, A., Alshurideh, M., Al Kurdi, B., & Salloum, S. A. (2020). Factors Influencing Electronic Service Quality on Electronic Loyalty in Online Shopping Context: Data Analysis Approach. In (Vol. NA, pp. 367-378). https://doi.org/10.1007/978-3-030-52067-0_16

Al Kurdi, B., Alshurideh, M., & Al afaishat, T. (2020). Employee retention and organizational performance: Evidence from banking industry. *Management Science Letters*, *10*(16), 3981-3990. https://doi.org/10.5267/j.msl.2020.7.011

Al Shebli, K., Said, R. A., Taleb, N., Ghazal, T. M., Alshurideh, M., & Alzoubi, H. M. (2021). AICV - RTA's Employees' Perceptions Toward the Efficiency of Artificial Intelligence and Big Data Utilization in Providing Smart Services to the Residents of Dubai. In (Vol. NA, pp. 573-585). https://doi.org/10.1007/978-3-030-76346-6_51

AlHamad, A. Q. M., Yaacob, N., & Al-Omari, F. (2012). Applying JESS rules to personalize Learning Management System(LMS)using online quizzes. *2012 15th International Conference on Interactive Collaborative Learning (ICL)*, *NA*(NA), 1-4. https://doi.org/10.1109/icl.2012.6402213

Ali, A., Septyanto, A. W., Chaudhary, I., Hamadi, H. A., Alzoubi, H. M., & Khan, Z. F. (2022). Applied Artificial Intelligence as Event Horizon Of Cyber Security. *2022 International Conference on Business Analytics for Technology and Security (ICBATS)*, *NA*(NA), NA-NA. https://doi.org/10.1109/icbats54253.2022.9759076

Alshamsi, M., Salloum, S. A., Alshurideh, M., & Abdallah, S. (2020). Artificial Intelligence and Blockchain for Transparency in Governance. In

(Vol. NA, pp. 219-230). https://doi.org/10.1007/978-3-030-51920-9_11

Alshurideh, M., Al Kurdi, B., & Salloum, S. A. (2019). *AISI - Examining the Main Mobile Learning System Drivers' Effects: A Mix Empirical Examination of Both the Expectation-Confirmation Model (ECM) and the Technology Acceptance Model (TAM)* (Vol. NA). https://doi.org/10.1007/978-3-030-31129-2_37

Alshurideh, M. T. (2022). Does electronic customer relationship management (E-CRM) affect service quality at private hospitals in Jordan? *Uncertain Supply Chain Management*, *10*(2), 325-332. https://doi.org/10.5267/j.uscm.2022.1.006

Alshurideh, M. T., Kurdi, B. A., Alzoubi, H. M., Obeidat, B., Hamadneh, S., & Ahmad, A. a. (2022). The influence of supply chain partners' integrations on organizational performance: The moderating role of trust. *Uncertain Supply Chain Management*, *10*(4), 1191-1202. https://doi.org/10.5267/j.uscm.2022.8.009

Alzoubi, H., & Ahmed, G. (2019). Do TQM practices improve organisational success A case study of electronics industry in the UAE. *International Journal of Economics and Business Research*, *17*(4), 459-NA. https://doi.org/10.1504/ijebr.2019.099975

Alzoubi, H. M., Ahmed, G., Al-Gasaymeh, A., & Al Kurdi, B. (2020). Empirical study on sustainable supply chain strategies and its impact on competitive priorities: The mediating role of supply chain collaboration. *Management Science Letters*, *10*(3), 703-708. https://doi.org/10.5267/j.msl.2019.9.008

Alzoubi, H. M., Alshurideh, M. T., Kurdi, B. A., Alhyasat, K. M. K., & Ghazal, T. M. (2022). The effect of e-payment and online shopping on sales growth: Evidence from banking industry. *International Journal of Data and Network Science*, *6*(4), 1369-1380. https://doi.org/10.5267/j.ijdns.2022.5.014

Alzoubi, H. M., Ghazal, T. M., Hasan, M. K., Alketbi, A., Kamran, R., Al-Dmour, N. A., & Islam, S. (2022). Cyber Security Threats on Digital Banking. *2022 1st International Conference on AI in Cybersecurity (ICAIC)*, *NA*(NA), NA-NA. https://doi.org/10.1109/icaic53980.2022.9896966

Barker, K. J., D'Amato, J., & Sheridon, P. (2008). Credit card fraud: awareness and prevention. *Journal of Financial Crime*, *15*(4), 398-410. https://doi.org/10.1108/13590790810907236

Bholat, D. (2015). Big Data and central banks. *Big Data & Society*, *2*(1), 2053951715579469-NA. https://doi.org/10.1177/2053951715579469

Bonsón, E., & Flores, F. (2011). Digital Transparency and Valuations of Social Media Compagnies. *Online*, *35*(3), 14-19. https://doi.org/NA

Chen, H., Chiang, R. H. L., & Storey, V. C. (2012). Business intelligence and analytics: from big data to big impact. *MIS Quarterly*, *36*(4), 1165-1188. https://doi.org/10.2307/41703503

Chui, K. T., Liu, R. W., Lytras, M. D., & Zhao, M. (2019). Big data and IoT solution for patient behaviour monitoring. *Behaviour & Information Technology*, *38*(9), 940-949. https://doi.org/10.1080/0144929x.2019.1584245

Dattaram, B. A., & Madhusudanan, N. (2016). Delay Prediction of Aircrafts Based on Health Monitoring Data. *International Journal of Business Analytics and Intelligence*, *4*(1), 29-37. https://doi.org/10.21863/ijbai/2016.4.1.015

El Khatib, M. M., Alzoubi, H. M., Ahmed, G., Kazim, H. H., Falasi, S. A. A. A., Mohammed, F., & Mulla, M. A. (2022). Digital Transformation and SMART-The Analytics factor. *2022 International Conference on Business Analytics for Technology and Security (ICBATS)*, *NA*(NA), NA-NA. https://doi.org/10.1109/icbats54253.2022.9759084

Fayyad, U. M., Grinstein, G., & Wierse, A. (2001). *Information Visualization in Data Mining and Knowledge Discovery* (Vol. NA). https://doi.org/NA

Fuller, M. (2015). Big Data: New science, new challenges, new dialogical opportunities. *Zygon®*, *50*(3), 569-582. https://doi.org/10.1111/zygo.12187

Gandomi, A. H., & Haider, M. (2015). Beyond the hype. *International Journal of Information Management*, *35*(2), 137-144. https://doi.org/10.1016/j.ijinfomgt.2014.10.007

Ghazal, T. M., Hasan, M. K., Alshurideh, M., Alzoubi, H. M., Ahmad, M., Akbar, S. S., Al Kurdi, B., & Akour, I. (2021). IoT for Smart Cities: Machine Learning Approaches in Smart Healthcare—A Review. *Future Internet*, *13*(8), 218-NA. https://doi.org/10.3390/fi13080218

Hanaysha, J. R., Al-Shaikh, M. E., Joghee, S., & Alzoubi, H. M. (2021). Impact of Innovation Capabilities on Business Sustainability in Small and Medium Enterprises. *FIIB Business Review*, *11*(1), 231971452110422-231971452110478. https://doi.org/10.1177/23197145211042232

Hasan, M., Popp, J., & Oláh, J. (2020). Current landscape and influence of big data on finance. *Journal of Big Data*, *7*(1), 1-17. https://doi.org/10.1186/s40537-020-00291-z

Hasan, S., O'Riain, S., & Curry, E. (2012). DEBS - Approximate semantic matching of heterogeneous events. *Proceedings of the 6th ACM International Conference on Distributed Event-Based Systems*, *NA*(NA), 252-263. https://doi.org/10.1145/2335484.2335512

Hoffmann, A. O. I., & Birnbrich, C. (2012). The impact of fraud prevention on bank-customer relationships: an empirical investigation in retail banking. *International Journal of Bank Marketing*, *30*(5), 390-407. https://doi.org/10.1108/02652321211247435

Kahn, B. K., Strong, D. M., & Wang, R. Y. (2002). Information quality benchmarks: product and service performance. *Communications of the ACM*, *45*(4), 184-192. https://doi.org/10.1145/505248.506007

Kaisler, S. H., Armour, F., Espinosa, J. A., & Money, W. H. (2013). HICSS - Big Data: Issues and Challenges Moving Forward. *2013 46th Hawaii International Conference on System Sciences*, *NA*(NA), 995-1004. https://doi.org/10.1109/hicss.2013.645

Lee, J.-C., & Chen, X. (2022). Exploring users' adoption intentions in the evolution of artificial intelligence mobile banking applications: the intelligent and anthropomorphic perspectives. *International Journal of Bank Marketing*, *40*(4), 631-658. https://doi.org/10.1108/ijbm-08-2021-0394

Lee, K. L., Romzi, P. N., Hanaysha, J. R., Alzoubi, H. M., & Alshurideh, M. (2022). Investigating the impact of benefits and challenges of IOT adoption on supply chain performance and organizational performance: An empirical study in Malaysia. *Uncertain Supply Chain Management*, *10*(2), 537-550. https://doi.org/10.5267/j.uscm.2021.11.009

Madakam, S., Holmukhe, R. M., & Jaiswal, D. K. (2019). The Future Digital Work Force: Robotic Process Automation (RPA). *Journal of Information Systems and Technology Management*, *16*(1), 1-17. https://doi.org/10.4301/s1807-1775201916001

Mahi, R. (2024). Optimizing supply chain efficiency in the manufacturing sector through ai-powered analytics. *International Journal of Management Information Systems and Data Science*, *1*(1), 41-50.

Muheidat, F., Patel, D., Tammisetty, S., Tawalbeh, L. a. A., & Tawalbeh, M. (2022). Emerging Concepts Using Blockchain and Big Data. *Procedia Computer Science*, *198*(NA), 15-22. https://doi.org/10.1016/j.procs.2021.12.206

O'Brien, S. P. (2010). Crisis Early Warning and Decision Support: Contemporary Approaches and Thoughts on Future Research. *International Studies Review*, *12*(1), 87-104. https://doi.org/10.1111/j.1468-2486.2009.00914.x

Rahaman, M., & Bari, M. (2024). Predictive Analytics for Strategic Workforce Planning: A Cross-Industry Perspective from Energy and Telecommunications. *International Journal of Business Diplomacy and Economy*, *3*(2), 14-25.

Rasouli, M. R. (2019). An architecture for IoT-enabled intelligent process-aware cloud production platform: a case study in a networked cloud clinical laboratory. *International Journal of Production Research*, *58*(12), 3765-3780. https://doi.org/10.1080/00207543.2019.1634847

Sadok, H., Sakka, F., & El Maknouzi, M. E. H. (2022). Artificial intelligence and bank credit analysis: A review. *Cogent Economics & Finance*, *10*(1), NA-NA. https://doi.org/10.1080/23322039.2021.2023262

Skyrius, R., Katin, I., Kazimianec, M., Nemitko, S., Rumšas, G., & Žilinskas, R. (2016). Factors Driving Business Intelligence Culture. *InSITE Conference*, *13*(NA), 171-186. https://doi.org/10.28945/3420

Shamim, M.M.I. (2024) "Artificial Intelligence in Project Management: Enhancing Efficiency and Decision-Making", *International Journal of Management Information Systems and Data Science*, 1(1), pp. 1–6. https://doi.org/10.62304/ijmisds.v1i1.107

Sun, Y., Shi, Y., & Zhang, Z. (2019). Finance Big Data: Management, Analysis, and Applications. *International Journal of Electronic Commerce*, *23*(1), 9-11. https://doi.org/10.1080/10864415.2018.1512270

Tariq, E., Alshurideh, M., Akour, I., & Al-Hawary, S. (2022). The effect of digital marketing capabilities on organizational ambidexterity of the information technology sector. *International Journal of Data and Network Science*, *6*(2), 401-408. https://doi.org/10.5267/j.ijdns.2021.12.014

Varian, H. R. (2014). Big Data: New Tricks for Econometrics. *Journal of Economic Perspectives*, *28*(2), 3-28. https://doi.org/10.1257/jep.28.2.3

Wei, W., Li, J., Cao, L., Ou, Y., & Chen, J. (2012). Effective detection of sophisticated online banking fraud on extremely imbalanced data. *World Wide Web*, *16*(4), 449-475. https://doi.org/10.1007/s11280-012-0178-0

Zhang, W., Zhong, J., Yang, S., Gao, Z., Hu, J., Chen, Y., & Yi, Z. (2019). Automated identification and grading system of diabetic retinopathy using deep neural networks. *Knowledge-Based Systems*, *175*(NA), 12-25. https://doi.org/10.1016/j.knosys.2019.03.016