# SECURE AND INCLUSIVE UTILIZATION OF SHARED DATA POTENTIAL WITH MULTI-KEY HOMOMORPHIC ENCRYPTION IN BANKING INDUSTRY

**Adang Haryaman[1*], Nyoman Dwika Ayu Amrita [2], Finny Redjeki [3]**

[1] Universitas Logsitik dan Bisnis , Bandung, 45363, Indonesia, Adang@ulbi.ac.id
[2] Universitas Ngurah Rai, Denpasar, 80238, Indonesia, dwika.ayu@unr.ac.id
[3] Universitas Sangga Buana YPK, Bandung, 40124, Indonesia, Finnyredjeki66@gmail.com

## Abstract

The use of multi-key homomorphic encryption (MHE) has become an important topic in the modern banking industry to improve data security and support secure information exchange between financial institutions. This technology allows mathematical operations to be performed on encrypted data without the need to decrypt it first, maintaining the confidentiality of sensitive information during the data analysis and processing process. This study discusses the potential impact of the use of MHE on operational efficiency, risk management and financial inclusion in the banking industry. First, MHE delivers advantages in operational efficiency by enabling banks to compute encrypted data, reducing the risk of data leaks and increasing system responsiveness. Second, the technology supports better risk management by facilitating anonymized data analysis, enabling banks to identify risk patterns and trends without compromising individual privacy. Third, MHE supports financial inclusion by enabling the development of more inclusive, anonymous data-based credit assessment models, opening up access to financial services to those previously difficult to reach. However, the widespread adoption of MHE is faced with several challenges, including high computational load and interoperability issues between different technology platforms. Solutions to address these challenges include the development of more efficient encryption algorithms, investment in IT infrastructure that can handle homomorphic workloads, and industry standardization and collaboration to facilitate effective MHE integration across financial institutions. In conclusion, by harnessing the potential of MHE and overcoming existing technical and regulatory challenges, the banking industry can strengthen data security systems, improve operational efficiency, and support financial inclusion in a more responsive and inclusive way.

Keywords: Multi-Key Homomorphic Encryption, Data Security, Operational Efficiency, Financial Inclusion

## INTRODUCTION

In the digital age, the banking industry stands at the forefront of innovation, leveraging technological advancements to enhance operational efficiency, improve customer experiences, and ensure robust security measures. One of the pivotal advances in this landscape is the adoption of multi-key homomorphic encryption (MHE), a sophisticated cryptographic technique that

enables secure data processing while maintaining privacy and confidentiality. This technology holds immense promise for revolutionizing how banks handle and utilize shared data, facilitating a more inclusive financial ecosystem that prioritizes both security and accessibility.

Homomorphic encryption, in its essence, allows computations to be performed on encrypted data without decrypting it first. This capability is particularly significant in banking, where sensitive financial information must be protected against unauthorized access and breaches. Traditional encryption methods typically require data to be decrypted before any computation can be performed, thereby exposing it to potential vulnerabilities. MHE, however, enables banks to conduct operations directly on encrypted data, preserving its confidentiality throughout various processing stages. This ability to perform secure computations on encrypted data sets MHE apart as a transformative technology for the banking industry.

The integration of MHE into banking operations promises several key benefits. Firstly, it enhances data privacy by ensuring that sensitive information remains encrypted throughout its lifecycle, from storage to analysis. This not only meets regulatory requirements but also builds trust among customers who expect their financial data to be handled with the utmost care. Second, MHE facilitates secure data sharing and collaboration between banks, fintech companies, and other stakeholders within the financial ecosystem. By enabling computations on encrypted data without exposing the underlying information, MHE supports collaborative efforts aimed at enhancing financial services and expanding market reach.

Moreover, MHE plays a crucial role in promoting financial inclusion by enabling banks to analyze anonymized data sets without compromising individual privacy. This capability is particularly relevant in developing economies where access to banking services is limited, and traditional credit scoring methods may not accurately reflect an individual's creditworthiness. By leveraging encrypted data for predictive analytics and risk assessment, banks can develop more inclusive lending practices and tailor financial products to meet the needs of underserved populations. This not only expands access to credit and other financial services but also fosters economic growth and stability within these regions.

Furthermore, the adoption of MHE supports compliance with stringent data protection regulations such as the General Data Protection Regulation (GDPR) in Europe or the California Consumer Privacy Act (CCPA) in the United States. These regulations impose strict requirements on how organizations handle and protect personal data, mandating measures to safeguard privacy and prevent unauthorized access. By implementing MHE, banks can demonstrate their

commitment to compliance while leveraging encrypted data for strategic insights and operational efficiencies.

In addition to its security and privacy benefits, MHE contributes to operational efficiency within banking institutions. By allowing computations to be performed on encrypted data in a secure environment, MHE reduces the need for data decryption and re-encryption processes, thereby streamlining operations and minimizing overhead costs. This efficiency gain is particularly advantageous in large-scale banking operations where vast amounts of data are processed daily, from transaction records and customer information to risk assessments and regulatory reporting.

However, despite its transformative potential, the widespread adoption of MHE in the banking industry faces several challenges. One significant barrier is the computational overhead associated with homomorphic operations, which can impact processing speed and resource utilization. Addressing these challenges requires ongoing research and development efforts to optimize encryption algorithms and enhance computational efficiency without compromising security. Additionally, ensuring interoperability between different encryption schemes and banking systems is crucial for facilitating seamless data exchange and collaboration across industry stakeholders.

Looking ahead, the future of multi-key homomorphic encryption in the banking industry hinges on continued innovation, collaboration, and regulatory alignment. As technological advances enable more efficient and scalable encryption solutions, banks can harness the full potential of encrypted data to drive innovation in financial services, enhance customer experiences, and achieve sustainable growth. By prioritizing security, privacy, and inclusivity, banks can position themselves at the forefront of digital transformation, setting new standards for data protection and ethical data usage in the global financial ecosystem.

## METHOD

This research adopts a desk study method to investigate the potential for secure and inclusive use of shared data using multi-key homomorphic encryption (MHE) in the banking industry. This approach involves an analysis of various relevant literature sources, including scientific journals, textbooks, research reports, and industry publications that discuss the application of homomorphic encryption technology in the context of banking data security and financial inclusion. The literature study begins with the identification and selection of appropriate information sources that cover key concepts such as homomorphic encryption, data security, and financial inclusion. This research aims to understand how MHE enables secure data processing without compromising

individual privacy, as well as how this technology can be used to facilitate collaboration and secure data exchange between financial institutions and other stakeholders.

The next step in this method is an in-depth analysis of the selected literature, focusing on the main findings regarding the implementation of MHE in banking. This involves examining the advantages of this technology in maintaining data confidentiality, increasing operational efficiency, complying with strict data protection regulations, as well as supporting financial inclusion by enabling anonymized data analysis for more accurate credit risk assessment. Additionally, this research also identifies challenges and barriers that may be faced in the widespread adoption of MHE in the banking industry, such as the computational burden of homomorphic operations and interoperability challenges between different encryption schemes. Critical analysis of this literature provides deep insight into how the banking industry can overcome these obstacles through technological innovation and cross-sector collaboration.

In conclusion, the literature study method in this research provides a solid theoretical foundation for understanding the implications of using MHE in the banking industry from various perspectives, including data security, operational efficiency, regulatory compliance, and financial inclusion. By combining key findings from relevant literature, this research provides a comprehensive framework to inform policies and implementation strategies for homomorphic encryption technology in supporting sustainable growth and innovation in global financial services.

## DISCUSSION

### Implementation of multi-key homomorphic encryption (MHE) can improve data security in the banking industry and facilitate secure data exchange between financial institutions

The implementation of multi-key homomorphic encryption (MHE) has great potential to improve data security in the banking industry while facilitating secure data exchange between financial institutions. This technology provides innovative solutions to the growing security challenges of the digital era, where information confidentiality is crucial in maintaining customer trust and complying with increasingly stringent data protection regulations.

One of the main advantages of MHE is its ability to allow computing on encrypted data without the need to decrypt it first. In the banking context, where the sensitivity of financial data is high, this method offers an additional layer of protection by allowing operations such as calculations, analysis and other data processing to be performed securely on data that remains encrypted. This not only reduces the risk of unauthorized access or data breaches, but also allows financial

institutions to better safeguard customer privacy, in accordance with applicable security and regulatory standards.

The implementation of MHE in the banking industry also brings significant benefits in the context of secure data exchange between financial institutions. Collaboration and data exchange are important in facing current challenges such as financial fraud, money laundering and other cyber crimes which are increasingly complex and cross regional borders. With MHE, financial institutions can send encrypted data to each other for joint risk analysis or for other linkage purposes without having to compromise privacy or face the risk of data leaks during the process of exchanging sensitive information.

In addition, MHE implementation also supports compliance with strict data regulations, such as the General Data Protection Regulation (GDPR) in the European Union or the California Consumer Privacy Act (CCPA) in the United States. This regulation sets strict requirements regarding the protection of personal data and requires organizations to take concrete steps to prevent unauthorized access and protect sensitive information. By using MHE, financial institutions can ensure that customers' personal and financial data remains protected throughout its lifecycle, from storage to use in analysis or processing.

However, MHE implementation does not come without challenges. One of the main issues that needs to be addressed is the computational overhead associated with homomorphic operations. Computational processes on encrypted data often require higher computing power compared to operations on unencrypted data, resulting in increased IT infrastructure costs and affecting overall system performance. Solutions to address these challenges include continued development in homomorphic encryption techniques to improve computational efficiency, as well as investment in more robust computing infrastructure to handle complex workloads.

Additionally, interoperability between various encryption schemes and banking platforms is also a key factor in the success of widespread MHE adoption. Involvement of multiple technology vendors, compatible encryption standards, and good system integration are key to ensuring that financial institutions can collaborate effectively and securely without compromising security or operational efficiency. Overall, the implementation of MHE as a solution to improve data security and facilitate secure data exchange in the banking industry shows great potential to change the paradigm in how sensitive information is managed and protected. By leveraging homomorphic encryption technology, financial institutions can not only meet stringent demands for data security and privacy, but also open new opportunities for more inclusive and efficient financial service innovation. Strategic steps to overcome technical challenges and optimize the

benefits of MHE will be key for financial institutions looking to exploit the full potential of this homomorphic encryption technology in the future.

**The potential impact of the use of MHE on operational efficiency and risk management in financial institutions**

The use of multi-key homomorphic encryption (MHE) has a significant potential impact on operational efficiency and risk management within financial institutions, while also supporting financial inclusion through anonymized data analysis. This technology not only improves data security, but also opens up new opportunities for more inclusive and efficient financial service innovation. First of all, in the context of operational efficiency, the use of MHE reduces the complexity associated with processing and processing sensitive data. Traditionally, to perform analysis or calculations on data, financial institutions must decrypt the information first, which can pose security risks and reduce time efficiency. With MHE, data remains encrypted during the analysis or calculation process, reducing the potential risk of data leaks and enabling faster and more efficient operations. For example, in a scenario where a bank needs to perform a risk analysis of an investment portfolio, MHE allows them to perform the necessary calculations without having to compromise the security of investors' personal data.

In addition, MHE also facilitates better risk management in financial institutions. With its ability to perform analysis on encrypted data, this technology allows banks to identify potential risk patterns and trends without compromising individual privacy. A concrete example of this is in credit scoring, where banks can use MHE to analyze clients' historical data without the need to reveal sensitive personal information. This not only strengthens data security, but also allows financial institutions to make decisions that are more accurate and responsive to changing market or economic conditions.

In parallel, the potential of MHE in supporting financial inclusion is enormous, especially through its ability to carry out anonymous data analysis. In many countries, access to financial services remains a challenge for a large portion of the population, especially those who do not have an established credit record or complete transaction history. By using MHE technology, financial institutions can analyze transaction data without having to personally identify the individuals involved. This paves the way for the development of alternative, more inclusive risk assessment models, which could expand access to credit and other financial products to those previously considered unreachable.

A concrete application example can be seen in the development of anonymous data-based alternative credit scores, where MHE allows banks to collect and analyze transaction data without affecting consumer privacy. In this context, banks can assess creditworthiness based on spending patterns or financial

behavior detected from encrypted data, without the need to reveal specific personal information. This not only promotes financial inclusion by expanding access to those previously difficult to provide services to, but also reduces bias and disparities in traditional credit assessment processes.

Additionally, the potential of MHE to support anonymous data analysis is also relevant in the context of increasingly stringent regulatory compliance. By maintaining data confidentiality, financial institutions can comply with strict data protection regulatory requirements, such as GDPR in Europe or CCPA in California, while still being able to leverage data for risk analysis and product innovation. This eliminates concerns about privacy breaches or data leaks that could result in legal sanctions and reputational harm for financial institutions.

However, there are several challenges that need to be overcome in adopting MHE to support operational efficiency and financial inclusion. One of these is the cost and technical complexity associated with implementing and managing infrastructure that supports MHE. Computational processes on encrypted data often require greater computing resources compared to operations on unencrypted data, which can increase operational costs and require investment in more sophisticated infrastructure.

Another challenge is the lack of uniformity in encryption schemes and interoperability between various technology platforms. The development of broader standards and frameworks for the integration of MHE with existing systems can help overcome these challenges and facilitate wider adoption in the global banking industry. This requires collaboration between technology providers, regulators and financial institutions to ensure that MHE can be implemented effectively and efficiently across global markets.

Overall, the potential impact of using MHE on operational efficiency and risk management within financial institutions, while also supporting financial inclusion through anonymized data analysis, shows great potential for a paradigm shift in the financial industry. By integrating these technologies with thoughtful business strategies and a commitment to continuous innovation, financial institutions can strengthen their position as leaders in safe, inclusive and sustainable financial services for all levels of society.

**The main challenges faced in the widespread adoption of MHE in the banking industry**

The widespread adoption of multi-key homomorphic encryption (MHE) in the banking industry faces a number of challenges that need to be overcome for this technology to provide maximum benefits in data security and operational efficiency. The two main challenges faced are the high computational load and interoperability problems between various technology platforms and systems.

First, high computational load is one of the main barriers to MHE adoption. Homomorphic encryption technology allows computations to be performed on encrypted data, which naturally results in an increase in computing power requirements. Mathematical operations performed on encrypted data often require greater computing resources than operations on unencrypted data. For example, multiplication or addition processes on encrypted data can generate significant overhead, slow system response times, and increase IT infrastructure costs.

One approach to overcome this computational challenge is to conduct further research in the development of more efficient homomorphic encryption algorithms. Some recent research has tried to increase the efficiency of homomorphic operations by optimizing encryption protocols or by developing new techniques such as the use of parallel computing techniques. The development of special chips or hardware optimized for homomorphic operations may also be a long-term solution to reduce the computational burden.

Apart from that, another approach to overcome the computational burden is to utilize cloud computing technology. Cloud computing services offer the ability to provision computing resources as needed, which can help reduce costs and increase the scalability of homomorphic operations. By using flexible cloud infrastructure, financial institutions can access greater computing power when needed for homomorphic operations without having to invest in expensive physical infrastructure.

The second significant challenge in the adoption of MHE in the banking industry is the issue of interoperability between various technology platforms and systems. Interoperability refers to the ability to integrate and operate effectively between different systems, applications, or technology platforms. In the MHE context, interoperability issues may arise due to different implementations of encryption protocols, security standards, or IT infrastructure between different financial institutions.

To overcome these interoperability challenges, there needs to be a standard framework or protocol that is widely accepted in the banking industry. Standardizing homomorphic encryption protocols can help ensure that systems from different financial institutions can communicate with each other and operate smoothly. Industry, regulators and technology providers need to collaborate to develop clear interoperability guidelines and practical solutions for integrating MHE in complex banking environments.

In addition, adequate training and education for IT and data security personnel in the use of MHE is also important to increase the level of understanding and technical skills required. Using homomorphic encryption technology requires in-depth knowledge of encryption protocols, key management, and complex data security principles. By increasing this understanding and skills

across the industry, financial institutions can reduce barriers to MHE implementation and exploit its potential more effectively.

Another approach to addressing interoperability issues is to leverage collaborative initiatives between financial institutions and technology providers. Strategic partnerships between large banks, fintechs and security technology service providers can help develop solutions that can be easily and securely integrated into existing IT infrastructure. This includes the development of open APIs or integration interfaces that facilitate secure and efficient data exchange between various platforms and systems.

Apart from computational and interoperability challenges, other aspects that need to be considered in the widespread adoption of MHE are regulatory and compliance aspects. Homomorphic encryption technology impacts the way financial institutions manage and protect sensitive data, requiring strict compliance with existing data protection regulations. For example, Europe's GDPR sets high standards regarding the use and protection of personal data, while other regulations may have different requirements depending on the jurisdiction and country.

To overcome these challenges, financial institutions need to ensure that their MHE implementation complies with applicable regulatory requirements. This includes adopting best practices in key management, security audits, and rigorous monitoring processes to ensure that data remains protected throughout its lifecycle. Active engagement with regulators and authorities is also important to ensure that their data security and privacy strategies are aligned with regulatory and policy evolution.

Overall, although the widespread adoption of multi-key homomorphic encryption (MHE) in the banking industry faces a number of significant challenges, the potential of this technology to improve data security, operational efficiency and support financial inclusion through anonymous data analysis is enormous. With the right approach to technology development, standardization, training, and regulatory compliance, financial institutions can overcome these barriers and maximize the benefits of using MHE in supporting sustainable growth and innovation in global financial services.

## CONCLUSION

In conclusion, the adoption of multi-key homomorphic encryption (MHE) offers great potential for the banking industry to improve data security, operational efficiency, and support financial inclusion through anonymous data analysis. Although this technology faces challenges such as high computational load and interoperability issues between systems, strategic steps can be taken to overcome these obstacles. The importance of developing more efficient

technologies and investing in supporting IT infrastructure, as well as standardizing homomorphic encryption protocols, can help accelerate widespread adoption of MHE across the banking industry. Additionally, intensive training for IT and data security personnel as well as strategic partnerships between financial institutions, fintechs and technology service providers are also important to ensure successful implementation. By taking these steps, financial institutions can not only strengthen their defenses against digital security threats, but also open the door to new innovations in safer, more inclusive and efficient financial services for society globally.

## BIBLIOGRAPHY


Aripin, Z., Fitrianti, NG, & Fatmasari, RR (2023). Digital Innovation and Knowledge Management: The Latest Approaches in International Business. A Systematic Literature Review in the Indonesian Context. *KRIEZ ACADEMY: Journal of development and community service* , *1* (1), 62-74.

Aripin, Z., Haryaman, A., & Sikki, N. (2024). INCENTIVE STRUCTURE AND ITS EFFECT ON REFERRALS: AN ANALYSIS OF THE ROLE OF SELF-CONSTRUCTION AS A DETERMINANT. *KRIEZ ACADEMY: Journal of development and community service* , *1* (2), 65-77.

Aripin, Z., Ichwanudin, W., & Faisal, I. (2023). BRAND SUSTAINABILITY STRATEGY DEVELOPMENT: THE ROLE OF SOCIAL MEDIA MARKETING AND MARKETING MANAGEMENT. *KRIEZ ACADEMY: Journal of development and community service* , *1* (1), 39-49.

Aripin, Z., Mulyani, SR, & Haryaman, A. (2023). MARKETING STRATEGY IN PROJECT SUSTAINABILITY MANAGEMENT EFFORTS IN EXTRACTIVE INDUSTRIES: BUILDING A RECIPROCITY FRAMEWORK FOR COMMUNITY ENGAGEMENT. *KRIEZ ACADEMY: Journal of development and community service* , *1* (1), 25-38.

Aripin, Z., Supriatna, U., & Mahaputra, MS (2023). WITH THE ADVENT OF CHATGPT: HOW TO IDENTIFY STRENGTHS, WEAKNESSES, OPPORTUNITIES, AND THREATS FOR THE FIELD OF EDUCATION AND THE BUSINESS WORLD OF VARIOUS DISCIPLINES. *KRIEZ ACADEMY: Journal of development and community service* , *1* (1), 50-61.

Aripin, Z., Supriatna, U., & Mahaputra, MS (2023). WITH THE ADVENT OF CHATGPT: HOW TO IDENTIFY STRENGTHS, WEAKNESSES, OPPORTUNITIES, AND THREATS FOR THE FIELD OF EDUCATION

AND THE BUSINESS WORLD OF VARIOUS DISCIPLINES. *KRIEZ ACADEMY: Journal of development and community service* , *1* (1), 50-61.

ARIPIN, Zaenal; REDJEKI, Finny; RUCHIYAT, Endang. THE EVOLUTION OF SALES ETHICS: ANALYSES OF THE PAST AND STRATEGIES FOR THE FUTURE. *Journal of Economics, Accounting, Business, Management, Engineering and Society*, 2024, 1.7: 16-28.

Chouhan, V., Ali, S., Sharma, R.B., & Sharma, A. (2023). The effect of financial technology (Fin-tech) on the conventional banking industry in India. *International Journal of Innovative Research and Scientific Studies* , *6* (3), 538-544.

Qi, R., Wang, J., Chang, R., & Shen, Y. (2021). The Impact of Financial Disintermediation on the Credit Business of Chinese Commercial Banks. *Open Journal of Social Sciences* , *9* (12), 288-298.

Pal, P. (2022). The adoption of waves of digital technology as antecedents of digital transformation by financial services institutions. *Journal of Digital Banking* , *7* (1), 70-91.

Bhandari, M. (2020). IMPORTANCE OF MARKETING RESEARCH: HOW TO CAPTURE MARKET INSIGHTS. *New Paradigms in management and social sciences* , 4.

Foxall, G. R. (2023). The neurophysiological behavioral perspective model and its contribution to the intentional behaviorist research program. *Frontiers in Human Neuroscience* .

REDJEKI, Finny; ARIPIN, Zaenal; RUCHIYAT, Endang. ANALYSING THE INFLUENCE OF INTERNET CELEBRITY SHORT VIDEOS ON VIEWER BEHAVIOUR: BEAUTY AS A PERSUASIVE FACTOR. *KRIEZ ACADEMY: Journal of development and community service*, 2024, 1.7: 31-44.

REDJEKI, Finny; ARIPIN, Zaenal; RUCHIYAT, Endang. ANALYSING THE INFLUENCE OF INTERNET CELEBRITY SHORT VIDEOS ON VIEWER BEHAVIOUR: BEAUTY AS A PERSUASIVE FACTOR. *KRIEZ ACADEMY: Journal of development and community service*, 2024, 1.7: 31-44.

REDJEKI, Finny; AMRITA, Nyoman Dwika Ayu; FAISAL, Ijang. IMPLICATIONS OF LOYALTY PROGRAMME COMPETITION ON CUSTOMER DECISIONMAKING IN THE BANKING INDUSTRY. *KRIEZ ACADEMY: Journal of development and community service*, 2024, 1.8: 1-16.

Redjeki, Finny. "Documentary Credit Sebagai Instrumen Perbankan Yang Dapat Memberikan Keamanan Pembayaran Bagi Pihak Eksportir Pada Perusahaan

Internasional." *Jurnal Techno-Socio Ekonomika Universitas Sangga Buana YPKP* 10.3 (2017): 248-259.

Redjeki, Finny, and Azhar Affandi. "Utilization of digital marketing for MSME players as value creation for customers during the COVID-19 pandemic." *International Journal of Science and Society* 3.1 (2021): 40-55.

Redjeki, Finny. "Documentary Credit Sebagai Instrumen Perbankan Yang Dapat Memberikan Keamanan Pembayaran Bagi Pihak Eksportir Pada Perusahaan Internasional." *Jurnal Techno-Socio Ekonomika Universitas Sangga Buana YPKP* 10.3 (2017): 248-259.

SJORAIDA, Diah Fatma; AMRITA, Nyoman Dwika Ayu; REDJEKI, Finny. COLLABORATION IN CREATING AN EDUCATIONAL CONSUMER JOURNEY: A MEANINGPERSPECTIVE FORMATION. *Journal of Economics, Accounting, Business, Management, Engineering and Society*, 2024, 1.8: 1-13.

Turner, A., Thomas, N., Menih, H., & Collins, A. (2024). Inner Peace: Evaluating a Complementary Program Promoting Intra-Personal Peace at Adelaide Women's Prison, Australia. *International journal of offender therapy and comparative criminology* , 0306624X241246099.

Dreyer, H., Sonnenberg, N., & Van der Merwe, D. (2022). Transcending linearity in understanding green consumer behavior: A social–cognitive framework for behavior changes in an emerging economy context. *Sustainability* , *14* (22), 14855.

Berkmann, M., Eisenbeiss, M., Reinartz, W., & Schauerte, N. (2024). Leveraging B2B field service technicians as a “second sales force”: how service situations affect selling activity and success. *Journal of the Academy of Marketing Science* , *52* (3), 736-761.

Razi, N., Moshabaki, A., Khodadad Hosseini, H., & Kordnaeij, A. (2022). A model for B2B salesperson performance with service ecosystems perspective: a grounded theory. *Journal of Business & Industrial Marketing* , *37* (6), 1314-1337.

Ohiomah, A., Benyoucef, M., & Andreev, P. (2020). A multidimensional perspective of business-to-business sales success: A meta-analytic review. *Industrial Marketing Management* , *90* , 435-452.

Bowen, M., Lai-Bennejean, C., Haas, A., & Rangarajan, D. (2021). Social media in B2B sales: why and when does salesperson social media usage affect salesperson performance?. *Industrial Marketing Management* , *96* , 166-182.

Elhajjar, S., Yacoub, L., & Ouaida, F. (2024). The present and future of the B2B sales profession. *Journal of Personal Selling & Sales Management* , *44* (2), 128-141.

Vanninen, J. (2022). *Customer-facing functions in B2B SaaS company business model design: how vendors configure sales, marketing, and customer success* (Master's thesis).

Høgevold, N., Rodriguez, R., Svensson, G., & Otero-Neira, C. (2021). B to B sellers' skill level in sales performance–frameworks and findings. *Journal of Business-to-Business Marketing* , *28* (3), 265-281.