International Journal of Economic Literature (INJOLE) e-ISSN: 3026-0221
Vol. 3 No. 4 April 2025, page., 263-275

E-COMMERCE APPLICATION DEVELOPMENT WITH SECURE PAYMENT METHOD INTEGRATION

Bekti Utomo *
Sekolah Vokasi, Universitas Sebelas Maret, Indonesia
E-mail: bektiutomo@staff.uns.ac.id

Kristiurman Jaya Mendrofa
Universitas Nias Raya, Indonesia
E-mail: kris@uniraya.ac.id

Loso Judijanto
IPOSS Jakarta, Indonesia
E-mail: losojudijantobumn@gmail.com

Abstract

This research discusses the development of e-commerce applications with the integration of secure payment methods. The focus of this literature is to analyze the various approaches and technologies used to ensure secure financial transactions in e-commerce platforms. In the current digital era, payment security is an important factor that influences user trust and comfort. Through a study of various literature sources and previous research, we found that encryption technology, tokenization, and compliance with industry standards such as PCI-DSS (Payment Card Industry Data Security Standard) play a key role in preventing fraud and protecting customer data. Additionally, diversification of payment methods to include credit/debit cards, e-wallets, and bank transfers, not only enhances security but also provides more flexibility for users. This research also highlights the importance of regular evaluations and audits to keep systems up-to-date with the latest threats. The conclusion of this study confirms that the integration of secure payment methods not only increases the level of customer trust and loyalty but also becomes a critical business strategy for the long-term sustainability of e-commerce platforms.

Keywords: E-Commerce, Secure Payment Methods, Encryption, Tokenization, PCI-DSS, Transaction Security, Application Development

INTRODUCTION

E-commerce application development has grown rapidly in this digital era, bringing a revolution in the way we shop and sell goods online. E-commerce applications present sophisticated solutions for business people to reach a wider market at relatively lower costs compared to traditional physical

stores. With easy navigation, extensive product catalogues, and personalized recommendations, e-commerce applications promise a shopping experience that is not only convenient but also adapts to each consumer's needs (Wu et al., 2022).

However, this growth also brings its own challenges, especially in terms of payment security. As the backbone of e-commerce activities, secure payment methods are very important to maintain consumer trust. Integration of payment methods that are not only safe, but also easy to use is a key factor in driving increased sales conversions and customer satisfaction. Therefore, e-commerce application developers must look for the best payment solutions that offer data security as well as confidentiality of customers' personal information (Sahoo & Chaurasiya, 2023).

Integrating secure payment methods in e-commerce applications requires a deep understanding of digital security aspects such as data encryption, two-factor authentication, and compliance with regulations such as the Payment Card Industry Data Security Standard (PCI DSS). Smooth payments and protection from the risk of personal information leakage or fraud are factors that can differentiate an e-commerce platform from its competitors (Mimani et al., 2024). Therefore, building a payment system must not only focus on technical aspects, but also consider the user experience so that it remains intuitive and does not eliminate security principles.

On theother hand, integration of payment methods must also respond to the dynamics of changing consumer behavior which is increasingly leading to non-cash transactions. Digital wallets, payments via mobile apps, on-the-go bank transfers, and contactless payments are some examples of modern payment methods that are expected to integrate seamlessly with e-commerce application systems. The availability and support for these various forms of payment shows flexibility and adaptation to continuously transforming market needs (Houcheimi & Mezei, 2024).

By prioritizing security and convenience, developing e-commerce applications with secure payment method integration has become a necessity in a competitive business environment (Zhou, 2024). Developers must work closely with cybersecurity experts and financial institutions to ensure that every transaction that occurs through their platforms is safe from cyber attacks. The entire online shopping process should not only make things easier for users, but also provide a sense of security that their finances and personal data are well protected (Jr. et al., 2022).

In the e-commerce application development process, choosing the right payment partner is a crucial step. A payment partner that has a good reputation and can provide comprehensive solutions will contribute significantly to the reputation and trust of the e-commerce brand itself. The selection of this partner must bebased on an analysis of thespecific needs of thetarget audienceas well as thetechnical capabilities possessed by the payment service provider (Zarichuk, 2024). Additionally, it is also important to consider the customer support offered and the extent of their flexibility in adapting new technology and evolving regulations.

Developing applications that integrate secure payment methods requires close collaboration between developers, UX designers, security analysts, and other stakeholders. The team must ensure that the user interface guides consumers through the payment process easily without complicating things (Niu et al., 2022). A balance between strong security and ease of use is key to producing a user-friendly interface. Intuitive design helps reduceuser errors and increases transaction speed and efficiency, which ultimately impacts customer satisfaction and loyalty to the platform (Xu, 2022).

Data analysis also plays an important role in increasing the effectiveness of payment methods in e-commerce applications. By leveraging big data and machine learning, developers can understand purchasing patterns, payment method preferences, and user behavior. This insight allows developers to continuously adjust and improvepayment features to offer services that are more personalized and tailored to consumer needs. Transaction security can be improved by identifying and preventing fraud attempts using advanced technologies such as analytical machine learning (Tan, 2024).

In a global context, e-commerceapplications must ensurethat their payment methods can operate across borders efficiently. This includes handling multiple currencies, complying with international financial regulations, and optimizing currency conversion rates. These things become especially relevant when facing a heterogeneous global market. The integration of international payment gateways and cryptocurrencies could be an alternative idea to answer global needs, providing more flexibility in the way consumers make payments that are not only safe but also inclusive (Wahaballa, 2022).

Through the development of e-commerce applications with the integration of secure payment methods designed with security, ease of use,

adaptability and a data-oriented approach in mind, e-commerce platforms can set new standards in the digital retail industry. This not only protects consumers and merchants, but also helps in strengthening the integrity and sustainability of the e-commerce ecosystem as a whole (Bago & Forgacs, 2023).

RESEARCH METHOD

The study in this research is qualitative with literature. The literature study research method is a research approach that involves the analysis and synthesis of information from various literature sources that are relevant to a particular research topic. Documents taken from literature research are journals, books and references related to thediscussion you want to research (Earley, M.A. 2014; Snyder, H. 2019).

RESULT AND DISCUSSION

Security Challenges Faced in Payment Transactions in Current E-Commerce Applications

In today's e-commerce ecosystem, online payment transactions face significant security challenges. One of the main challenges is the risk of payment fraud and identity theft. Cybercriminals are increasingly sophisticated in creating fraudulent schemes that deceive both buyers and sellers (Alam et al., 2024). For example, phishing, where fraudsters create fake payment pages to collect personal and financial information from victims. Additionally, man-in-the-middle (MITM) attacks allow fraudsters to intercept and manipulate information transmitted between buyers and e-commerce sites without both parties knowing.

Another issue that complicates payment security in e-commerce applications is the security of buyer data. Strict data protection laws in various jurisdictions require companies to implement robust data security measures to protect users' personal information. Data leaks can occur through security gaps in payment systems, cyberattacks against user databases, or through weaknesses in third-party data storage. Any leak of this information can cause huge financial losses for users and permanently damage the reputation of the e-commerce platform (Jha & Prashar, 2022).

Furthermore, another security challenge is integration with adequate payment methods. With the increasing number of payment methods available, from credit and debit cards to digital payments and cryptocurrencies, each method has specific vulnerabilities that need to be

addressed. Integrating these various methods into an e-commerce platform not only adds technical complexity but also expands potential security gaps. Security must be maintained at every integration point while ensuring that the payment process remains smooth and user-friendly for users (Banerjee, 2022).

To overcome these challenges, e-commerce providers must implement advanced security technologies, such as strong data encryption, two-factor authentication, and real-time transaction monitoring to detect and prevent suspicious activity (Shanmugasamy, 2024). In addition, user education about good security practices is also important, because the human factor is often a weak point in terms of security. Fostering cooperation between government, industry and consumers is the main key in strengthening the payment security ecosystem and protecting all parties from the risk of cybercrime in the world of e-commerce.

Facing payment security challenges in e-commerce applications is not easy, but maintaining consumer trust is irreplaceable. This effort requires continued investment in innovative security technologies and strict implementation of industry standards, such as the Payment Card Industry Data Security Standard (PCI DSS). This standard helps ensure that all entities that store, process, or transmit payment card information maintain a secure environment. The implementation of technologies such as tokenization and blockchain also offers thepromiseof increasing payment security by replacing sensitivedata with uniquetokens or recording transactions in an immutable form (Nicholas et al., 2023).

The importance of cross-sector collaboration cannot be ignored. Governments, regulators, the payments industry and e-commerce companies must work together to develop legal and policy frameworks that support innovation while curbing fraud and enhancing security. Initiatives such as stricter buyer authentication and restrictions on card-not-present fraud require collaboration between card issuers, payment networks, and retailers (Joshi, 2024).

From the perspective of an e-commerce platform developer, adopting "security from the start" principles in product development can make a significant difference. This involves designing systems with security considerations as a priority, not just an afterthought. Rigorous security testing, including penetration testing and regular vulnerability evaluation, should be a standard component of the product development cycle (Masood et al., 2023).

Effectiveness and Safe Payment Methods that Have Been Integrated in E-Commerce Applications

The effectiveness of payment methods integrated in e-commerce applications is oneof thekey factors that determinethesuccess of a platform. Ease of the payment process can increase user comfort, which has a direct impact on increasing sales conversion rates. Various payment methods provide flexibility for consumers to choose the payment method that is most comfortable and safe for them. Thus, e-commerce applications that are able to provide various payment options tend to be preferred by users compared to those that only offer limited options (Bansal et al., 2023).

Various payment methods that are commonly integrated in e-commerce applications include credit cards, bank transfers, e-wallets, and PayLater services. Credit cards offer flexibility and speed in transactions, while bank transfers provide additional security for customers who are still unsure about using credit cards (Liu, 2022). Meanwhile, e-wallets such as GoPay, OVO, and Dana are increasingly popular because of their ease of use and often offer special promos or discounts. Apart from that, the PayLater service provides installment or payment options at a later date which can attract more customers.

Security in the payment process is a crucial factor in maintaining consumer trust in e-commerce applications. The implementation of encryption technology and security protocols such as SSL (Secure Socket Layer) is a standard that must exist to protect user data during transactions. Additionally, multiple authentication (2FA) methods are increasingly commonly used to prevent unauthorized access. E-commerce platforms that adopt the PCI DSS (Payment Card Industry Data Security Standard) standard also demonstrate their commitment to maintaining the security of customer payment data, which in turn increases consumer trust (Kumar, 2022).

The overall effectiveness and security of payment methods integrated in e-commerceapplications greatly influences user experienceand thelevel of public trust. By continuing to innovate and adopt the latest technology in the field of payment security, e-commerce applications can provide maximum comfort and security for their users (Maheswari & Theivasakthi, 2023). Ultimately, applications that can harmonize payment process efficiency with a high level of security will bebetter able to retain customers and increase overall business growth.

Apart from that, adaptive and inclusive payment methods are also able to reach various different consumer segments. For example, payment

methods via e-wallet are often more popular with millennials and Gen Z who are used to digital technology. Meanwhile, conventional methods such as bank transfers or payments via physical outlets may be more suitable for consumers who are not very familiar with technology or do not have sufficient access to digital banking services. This diversification of payment methods allows e-commerce applications to reach various levels of society, thereby not limiting their market potential (Rashminda & Jayatissa, 2024).

Adoption of user-friendly payment methods can also increase customer loyalty. Customers who are satisfied with the easy and safe transaction process are likely to return to shop on the same platform in the future (Gopakumar et al., 2022). Additionally, e-commerce applications can integrate loyalty or rewards programs through certain payment methods, which can further increase user engagement. For example, collaboration with e-wallet providers to provide cashback or reward points for certain transactions can be an additional incentive for consumers.

In facing the challenges of the dynamic digital era, e-commerce applications must continue to develop and update their payment systems. Innovations such as biometric-based payments, such as fingerprint or facial recognition, are now starting to be adopted to provide an additional layer of security and convenience for users. Blockchain technology is also starting to be seen as a solution for better transaction transparency and security. By implementing these technologies, e-commerce applications can continue to compete and meet consumers' increasingly high expectations for transaction efficiency and security (Deng, 2024).

Overall, the effectiveness and security of payment methods integrated in e-commerce applications not only function as transaction tools, but also as strategic factors in building credibility and business sustainability. By ensuring reliable, secure and inclusive payment methods, e-commerce platforms are able to create positive transaction experiences for consumers (Chen, 2023). This in turn will increase customer loyalty and help e-commerce companies to remain competitive in an increasingly crowded and challenging market.

E-Commerce Application Development with Payment Method Integration that is Not Only Safe but Also User-Friendly

Modern e-commerce application development demands the integration of payment methods that not only prioritize security, but are also user-friendly. In this context, transaction security is a crucial element for building consumer trust. Data encryption technology and two-factor

authentication are some examples of technologies that can be implemented to ensure users' financial information is well protected (Gao et al., 2023). In addition, the introduction of biometric-based payment methods such as fingerprint or facial recognition also adds a layer of security which also makes the user identity validation process easier.

Apart from security aspects, comfort and ease of use are determining factors in the success of an e-commerce application. Diversifying payment methods is a strategy that can be implemented to reach various types of consumers. For example, providing payment options via e-wallet, credit card, bank transfer, to physical outlets will allow applications to better serve the needs of various market segments. Ensuring that all of these methods are easy to access and use through an intuitive user interface will improve the overall shopping experience, thereby driving conversion rates and customer loyalty (Yang et al., 2023).

The successful integration of safe and user-friendly payment methods in e-commerce applications can also be strengthened by value-added contribution programs such as cashback, discounts and reward points. Collaboration with payment service providers such as e-wallets to provide additional incentives for consumers could be a strategic step to increase the platform's attractiveness. By continuing to follow technological developments and market trends in terms of payment methods, e-commerce applications can remain relevant and competitive, while meeting user expectations regarding the convenience and security of digital transactions (Hwangbo, 2022).

After ensuring the integration of payment methods is safe and user-friendly, another important focus is optimizing the performance of the e-commerce application itself. A satisfactory user experience depends not only on security and ease of payment, but also on responsive and non-sluggish application performance. Utilizing cloud technology for scalability, caching data to speed up access, and conducting regular load testing are highly recommended. This will ensure the application can handle traffic spikes and provide a smooth, uninterrupted shopping experience (Sabit, 2022).

Apart from that, it is also important to pay attention to the personalization aspect in e-commerce applications. Users are more likely to engage and make purchases when they feel the app understands their needs. Machine learning algorithms and big data analytics can be used to analyze user shopping behavior and provide relevant product recommendations. Personalization features can include various elements such as lists of

recommended products, product availability notifications, and special offers tailored to each user's preferences (Parghi & Dodia, 2022).

No less important, responsive customer service is also key in maintaining user loyalty in e-commerce applications. Providing various communication channels, including live chat, email and call center, with fast responses and solutions will increase user satisfaction. Implementing an AI-based chatbot to answer frequently asked questions can be an efficient solution that provides additional convenience for users. With a holistic view that covers all these aspects, e-commerce applications can achieve sustainable success in an increasingly competitive digital market (Gupta, 2022).

CONCLUSION

Secure payment method integration ensures that sensitive data such as credit card information and customer personal data is protected from cyber threats. The use of technologies such as encryption and tokenization is an important step in achieving this goal. When users feel safe making transactions, they are more likely to make repeat purchases. Secure payment methods increase user trust in your e-commerce platform. A smooth and secure payment system makes it easier for customers to complete their transactions quickly and without obstacles. This contributes to increasing sales conversion rates. Offering a variety of payment methods, such as credit/debit cards, e-wallets, and bank transfers, provides greater flexibility for users. It also reaches more market segments and user preferences. Complying with industry standards such as PCI-DSS (Payment Card Industry Data Security Standard) is not only important for security, but also to ensure business operations comply with applicable regulations.

The use of secure payment methods also requires regular evaluation and audits to ensure the system remains up-to-date and complies with the latest security standards. Good payment security increases customer loyalty. Users who feel safe are more likely to return and recommend the platform to others. A secure and efficient payment system reduces issues such as failed transactions and payment disputes, ultimately reducing operational burdens and allowing focus on developing other value-adding features. Integration of secure payment methods in e-commerce application development is a crucial factor that not only ensures security and regulatory compliance, but also improves user experience and trust. Thus, investing in secure payment solutions is not only a wise move for protection, but also an important strategy for long-term business success.

REFERENCES

Alam, S. S., Ahmed, S., Kokash, H. A., Mahmud, Md. S., & Sharnali, S. Z. (2024). Utility and hedonic perception- Customers' intention towards using of QR codes in mobile payment of Generation Y and Generation Z. *Electronic Commerce Research and Applications*, *65*(Query date: 2024-09-10 19:21:22), 101389–101389. https://doi.org/10.1016/j.elerap.2024.101389

Bago, P., & Forgacs, B. (2023). Integration of the Instant Payment System into Hungary's Payment Infrastructure. *SSRN Electronic Journal*, *Query date: 2024-09-10 19:27:18*. https://doi.org/10.2139/ssrn.4362385

Banerjee, A. (2022). The Impact of Soft Robotics In Today's World: Applications, Challenges Faced, And Future Outlook. *2022 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON)*, *Query date: 2024-09-10 19:21:22*. https://doi.org/10.1109/smartgencon56628.2022.10084295

Bansal, A., Khosla, T., & Saini, V. K. (2023). Security Challenges and various methods for Increasing Security in E-Commerce Applications. *International Journal for Research in Applied Science and Engineering Technology*, *11*(1), 311–316. https://doi.org/10.22214/ijraset.2023.48475

Chen, H. (2023). *Life Challenges Faced By Chinese Workers In Africa*. *Query date: 2024-09-10 19:21:22*. https://doi.org/10.47611/harp.303

Deng, L. (2024). Multi-agent Secure Payment Model of E-commerce Based on Blockchain Perspective. *International Journal of Information and Computer Security*, *24*(1). https://doi.org/10.1504/ijics.2024.10065234

Earley, M. A. (2014). A synthesis of the literature on research methods education. Teaching in Higher Education, 19(3), 242-253.

Gao, W., Guo, Q., & Jiang, N. (2023). Information vulnerability in facial recognition payment: An explanation of technology threat avoidance and information boundary theory. *Electronic Commerce Research and Applications*, *61*(Query date: 2024-09-10 19:21:22), 101298–101298. https://doi.org/10.1016/j.elerap.2023.101298

Gopakumar, K., Suresh, M., & Dutta, P. (2022). Operational Challenges Faced by E-Commerce Industry During COVID-19 Era. *World Scientific Series in Asian Business and Management Studies*, *Query date: 2024-09-10 19:21:22*, 277–293. https://doi.org/10.1142/9789811245992_0014

Gupta, Dr. S. (2022). E-commerce Payment Security Strategies for Online Payments. *Kaav International Journal of Law, Finance & Industrial Relations*, *Query date: 2024-09-10 19:21:22*. https://doi.org/10.52458/23492589.2022.v9.iss1.kp.a2

Houcheimi, A., & Mezei, J. (2024). The Role of Secure Online Payments in Enabling the Development of E-Tailing. *Journal of Organizational*

Computing and Electronic Commerce, *Query date: 2024-09-10 19:27:18*, 1–19. https://doi.org/10.1080/10919392.2024.2371236

Hwangbo, Y. (2022). Government Challenges Over Global Electronic Commerce Using FinTech. *Advances in Finance, Accounting, and Economics*, *Query date: 2024-09-10 19:21:22*, 197–213. https://doi.org/10.4018/978-1-7998-8447-7.ch011

Jha, N., & Prashar, D. (2022). Using Blockchain in Resolving the Challenges Faced by IIoT. *Industrial Internet of Things*, *Query date: 2024-09-10 19:21:22*, 189–216. https://doi.org/10.1201/9781003102267-11

Joshi, P. K. (2024). Spring Boot Security in Payment Gateway Applications. *International Journal of Computing and Engineering*, *6*(4), 13–21. https://doi.org/10.47941/ijce.2201

Jr., O. L. C. R., Lucena, B. R. D., Souza, A. L. de, & Poleto, T. (2022). The Evolution of Community Development Banks Influenced by E-Payment and Its Social Impact on Brazil. *Advances in Electronic Commerce*, *Query date: 2024-09-10 19:27:18*, 229–249. https://doi.org/10.4018/978-1-7998-9035-5.ch013

Kumar, D. (2022). Prospects and Challenges of Mobile Financial Services (MFS) in Bangladesh. *Advances in Electronic Commerce*, *Query date: 2024-09-10 19:21:22*, 320–341. https://doi.org/10.4018/978-1-7998-9035-5.ch017

Liu, S. (2022). Reliability Evaluation Method of Mobile Payment E-commerce System based on Support Vector Machine. *2022 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA)*, *Query date: 2024-09-10 19:21:22*, 51–57. https://doi.org/10.1109/aeeca55500.2022.9918835

Maheswari, E., & Theivasakthi, P. A. (2023). Problems and challenges faced by women entrepreneurs in Surandai, Tenkasi district. *I-Manager's Journal on Economics & Commerce*, *3*(3), 25–25. https://doi.org/10.26634/jecom.3.3.20584

Masood, M., Asfia, Y., & Khawaja, S. G. (2023). Security Challenges Faced by RISC-V open-source Processors and its Security Features: A Survey. *2023 25th International Multitopic Conference (INMIC)*, *12*(Query date: 2024-09-10 19:21:22), 1–7. https://doi.org/10.1109/inmic60434.2023.10465851

Mimani, S., Ramakrishnan, R., Rohella, P., Jiwani, N., & Logeshwaran, J. (2024). The Utilization of AI Extends Beyond Payment Systems to E-Commerce Store Development. *2024 2nd International Conference on Disruptive Technologies (ICDT)*, *11*(Query date: 2024-09-10 19:27:18), 555–560. https://doi.org/10.1109/icdt61202.2024.10489393

Nicholas, J., Ruben, G., & Meiryani. (2023). The Effect of Paylater Payment Method on Impulsive Buying of E-Commerce Users in Indonesia. *2023 International Conference on Digital Applications, Transformation & Economy (ICDATE)*, *5*(Query date: 2024-09-10 19:21:22), 1–6. https://doi.org/10.1109/icdate58146.2023.10248527

Niu, B., Dong, J., Dai, Z., & Liu, Y. (2022). Sales data sharing to improve product development efficiency in cross-border e-commerce. *Electronic Commerce Research and Applications*, *51*(Query date: 2024-09-10 19:27:18), 101112–101112. https://doi.org/10.1016/j.elerap.2021.101112

Parghi, V. K., & Dodia, B. M. (2022). Electronic Payment Systems: Security Issues and Solutions. *Darshan - The International Journal of Commerce and Management (DIJCM)*, *2*(1), 22–30. https://doi.org/10.56360/dijcm/1.i.2022.2204

Rashminda, L., & Jayatissa, Y. (2024). Payment and Security Concerns in Sri Lankan E-Commerce Web Sites. *2024 International Research Conference on Smart Computing and Systems Engineering (SCSE)*, *18*(Query date: 2024-09-10 19:21:22), 1–6. https://doi.org/10.1109/scse61872.2024.10550871

Sabit, K. (2022). Ensuring Food Security in Nigeria: Remedies to the Challenges Being Faced by the Populace. *SSRN Electronic Journal*, *Query date: 2024-09-10 19:21:22*. https://doi.org/10.2139/ssrn.4108882

Sahoo, S. S., & Chaurasiya, V. K. (2023). VIBE: Blockchain-based Virtual Payment in IoT Ecosystem: A Secure Decentralized Marketplace. *Multimedia Tools and Applications*, *83*(6), 16869–16894. https://doi.org/10.1007/s11042-023-15634-0

Shanmugasamy, K. (2024). The Future of Transactions: Exploring the Impact and Applications of Intelligent Payment Systems. *International Journal of Science and Research (IJSR)*, *13*(9), 158–161. https://doi.org/10.21275/sr24901223954

Snyder, H. (2019¬). Literature review as a research methodology: An overview and guidelines. Journal of business research, 104, 333-339.

Tan, H. (2024). Logistics Services, E-payment Systems, and After-sales Support Integration: Basis for Strategic Framework for Enhancing Cross-border E-commerce. *Frontiers in Business, Economics and Management*, *16*(1), 415–426. https://doi.org/10.54097/zsr9b847

Wahaballa, A. (2022). *Lightweight and Secure IoT-based Payment Protocols from an Identity-Based Signature Scheme*. *Query date: 2024-09-10 19:27:18*. https://doi.org/10.20944/preprints202210.0331.v1

Wu, M., Liu, Y., Chung, H. F. L., & Guo, S. (2022). When and how mobile payment platform complementors matter in cross-border B2B e-commerce ecosystems? An integration of process and modularization analysis. *Journal of Business Research*, *139*(Query date: 2024-09-10 19:27:18), 843–854. https://doi.org/10.1016/j.jbusres.2021.10.019

Xu, R. (2022). Optimized Secure Payment Solution Using QR Code Scanning based on Operation-payment Dual Devices. *BCP Business & Management*, *17*(Query date: 2024-09-10 19:27:18), 118–123. https://doi.org/10.54691/bcpbm.v17i.383

Yang, M., Jiang, J., Cameron, A.-F., & Liu, X. (2023). How do you cope? Online medical consultation service uncertainty, coping strategies, and subsequent payment. *Electronic Commerce Research and Applications*, *61*(Query date: 2024-09-10 19:21:22), 101294–101294. https://doi.org/10.1016/j.elerap.2023.101294

Zarichuk, O. (2024). Security in cloud computing: Methods for ensuring privacy and integration in modern applications. *Development Management*, *23*(1), 37–45. https://doi.org/10.57111/devt/1.2024.37

Zhou, Y. (2024). The Impact of Payment Methods on Consumer Behavior in the E-commerce Environment. *International Journal of Web Based Communities*, *20*(3). https://doi.org/10.1504/ijwbc.2024.10061791