JOURNAL OF APPLIED INTELLIGENT SYSTEMS & INFORMATION SCIENCES

VOL. 4, ISSUE 2, PP. 52-60, DECEMBER 2023.
Available at: https://journal.research.fanap.com/
DOI: https://doi.org/10.22034/JAISIS.2023.418932.1072

MITIGATING DATA LOSS AND ITS IMPACT ON MODERN SOFTWARE ENGINEERING: A CASE STUDY APPROACH

Leila Pakravan Nejad [1,*]

[1] *Digital Banking Department, Dotin Co., Tehran, Iran.*

ABSTRACT

In today's business environment, the increasing reliance on information systems has become vital, driving operational efficiency across various sectors. However, this dependence comes with a critical concern - the looming threat of data loss. This paper delves into the intricate challenges associated with data loss in the realm of software engineering, specifically its implications for software companies managing essential databases. The consequences of data loss incidents, which encompass financial setbacks and harm to reputation, have far-reaching consequences for organizations dealing with sensitive data. The core focus following a data loss event is rapid and effective recovery to minimize disruptions and curtail losses. A range of recovery techniques, such as backups, redundancy measures, replication approaches, and comprehensive disaster recovery plans, are explored. This paper thoroughly examines the intricate interplay between information systems, data vulnerability, recovery strategies, and preventive actions. By conducting a comprehensive assessment of data loss scenarios and recovery methodologies, this paper aims to offer holistic insights into the significance of preventing data loss in today's digital landscape. Additionally, the paper presents a case study that demonstrates the complex nature of responding to incidents, analyzing root causes, prioritizing solutions, and adopting an optimal approach to mitigate the ramifications of data loss incidents.

KEYWORDS: Data loss, Information system, Recovery, Data protection, Software engineering

1. INTRODUCTION

The reliance on information systems has grown substantially in the modern business landscape, facilitating efficient operations across various sectors. However, this reliance comes with a potential peril the risk of data loss. The stakes are high for organizations dealing with sensitive data such as financial records and customer information. Data loss incidents can lead to severe consequences, encompassing financial losses, legal liabilities, reputation damage, and customer trust erosion (Luo & Zahra, 2023; Vučinić & Luburić, 2022).

Data loss represents a critical challenge in software engineering, particularly for software companies managing extensive databases. These databases house vital customer data, financial records, and transaction histories that are crucial for seamless operations. Any form of data loss can result in significant disruptions, legal ramifications, and even business closure. The central objective after a data loss incident is recovery. Swift

* *Corresponding Author, Email: l.pakravan@dotin.ir*

RECEIVED: 01 OCTOBER 2023; **ACCEPTED**: 25 DECEMBER 2023; **PUBLISHED ONLINE**: 25 DECEMBER 2023

and effective recovery minimizes disruptions, ensures data availability, and mitigates potential financial and reputational losses. Companies employ various recovery methods, including regular backups, redundancy measures, replication techniques, and comprehensive disaster recovery plans to achieve this. Software companies must adopt a multifaceted approach to prevent the loss of valuable data. This approach includes investing in robust infrastructure, performing routine maintenance and testing, implementing stringent data security measures, and educating employees about data protection. By embracing these strategies, companies can significantly reduce the risk of data loss and ensure a swift and secure recovery in case of any unfortunate incidents (Ghelani et al., 2022; Khan et al., 2022; Khiaonarong et al., 2021; OECD, 2021; Ramzan et al., 2022).

This paper investigates the critical realm of data loss in software engineering, focusing on the intricate interplay between information systems, data vulnerability, recovery methods, and preventive measures. We also explore real-world use cases, analyzing a scenario where data loss within a software company's banking solutions unit led to severe consequences, underscoring the urgency of proactive data protection strategies. Through a comprehensive examination of data loss scenarios, recovery techniques, and preventive strategies, this paper aims to provide a holistic understanding of the significance of data loss prevention (DLP) in the modern digital landscape. Based on this objective, the paper is organized as follows. The methods and factors that influence data loss recovery and prevention are investigated in Section 2. In Section 3, the effects of data loss on the company and customer are examined. Different aspects of the issue within the considered case study are scrutinized in Section 4, and the concluding remarks are presented in Section 5.

2. DATA LOSS RECOVERY AND PREVENTION

Data loss refers to the unintended or accidental removal, corruption, or destruction of data stored in a database. A software company with thousands of customers could lose critical customer information, financial data, transaction records, user profiles, application settings, and other valuable data. This loss can occur for various reasons, such as hardware failures, software bugs, cyberattacks, human errors, and natural disasters. The primary purpose of preventing data loss is to ensure the continuity of business operations, protect sensitive data, maintain customer trust, and minimize financial and reputational damages. Software companies rely heavily on accurate and secure data storage to provide their services effectively. Losing this data could lead to service disruptions, regulatory compliance issues, legal liabilities, and erosion of customer confidence (Khan et al., 2016; Lehto, 2022; Liu & Yu, 2022; Arogundade, 2023; Singhal, 2022; Tari et al., 2023). In this regard, we examine data recovery and DLP.

2.1. Methods for Data Recovery

Among the factors and methods that can recover sensitive data, the following can be mentioned:

- Regular Backups: Regularly backing up the database is crucial. Backups create copies of the data at specific points in time. In case of data loss, the database can be restored to a previous state using these backups. It is important to ensure that backups are performed frequently and are stored securely.
- Replication: Implementing database replication can help maintain redundant copies of data on separate servers. If one server fails, another can take over, minimizing downtime. Replicating the database across multiple servers or locations can help prevent data loss. This ensures that even if one system fails, the data is still available on another system.
- Point-in-Time Recovery: This involves restoring the database to a specific point in time before the data loss occurred. It is useful for recovering data without affecting the most recent transactions.
- Data Recovery Tools: Specialized software tools can sometimes help recover data from damaged or corrupted databases.
- Cloud Services: Many cloud providers offer built-in data recovery and backup solutions if the company uses cloud-based infrastructure.

- Database Auditing: Regularly auditing and monitoring the database can help detect anomalies and potential issues before they lead to data loss.
- Disaster Recovery Plan: A well-defined disaster recovery plan ensures that the organization knows how to respond to data loss incidents promptly and effectively promptly and effectively.
- Redundancy and fault tolerance: Implementing redundancy measures, such as redundant storage systems, can help minimize the impact of hardware failures. Using fault-tolerant systems ensures that data remains accessible even if specific components fail.

2.2. Data Loss Prevention

Similar to the factors for data recovery, data loss can be prevented by using factors similar to the following (Fig. 1 for more details):

- Redundancy: Implementing redundancy by having multiple servers and backups can ensure that even if one system fails, others are ready to take over.
- Regular Backups: Scheduled and frequent backups help create restore points that reduce the impact of data loss.
- Data Validation and Error Handling: Robust software engineering practices should include proper data validation and comprehensive error handling to prevent data corruption and loss.
- Access Control: Implement strict access controls and authentication mechanisms to prevent unauthorized access that could lead to data loss.
- Security Measures: Implement cybersecurity measures like firewalls, intrusion detection systems, and encryption to safeguard against cyberattacks.
- Employee Training: Educate employees about best practices, security protocols, and the importance of data protection to minimize human errors.
- Disaster Recovery Plan: Develop and maintain a comprehensive disaster recovery plan that outlines procedures for responding to data loss incidents.
- Robust infrastructure: Invest in reliable and secure hardware and software systems that can withstand failures and minimize the risk of data loss.
- Regular maintenance and testing: Perform routine system maintenance and testing to identify and address vulnerabilities before they lead to data loss. This includes regular software updates, patching, and security audits.

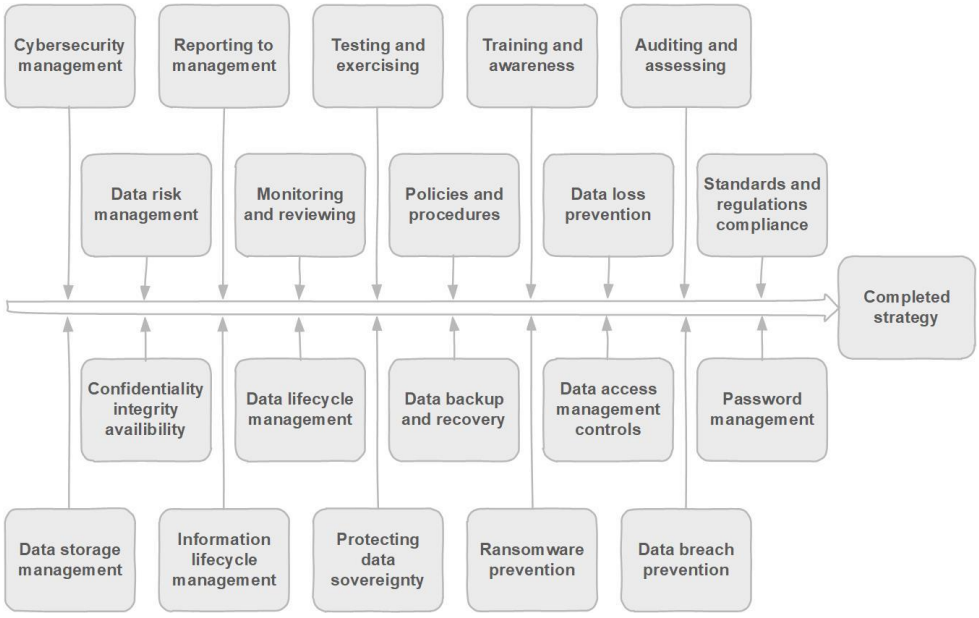

Fig. 1. Data protection strategy

3. EFFECTS ON THE COMPANY AND CUSTOMER

The problems discussed earlier can have implications that extend to both customers and software companies, imposing specific limitations. Consequently, these limitations can give rise to a range of potential consequences in connection with the issue of data loss:

3.1. Customer Loss

Among the effects of data loss for the customer, the following can be mentioned (De Mesquita et al., 2023; Marhaeni et al., 2023; Mpofu, 2022; Tripp et al., 2022):

- Financial Loss: Customers in the middle of transactions during the system failure might experience actual financial losses. Funds could be deducted from their accounts without receiving goods or services, or deposits might not have been processed. This can have significant financial implications for customers.
- Trust and Confidence Erosion: The failure of the switching system and subsequent loss of transaction data erodes customer trust and confidence in the bank's ability to manage their financial transactions securely and reliably. Such incidents can lead customers to doubt the overall safety of their accounts and transactions. When a bank's systems fail to handle transactions properly, it erodes trust. Customers may begin to doubt the bank's ability to protect their financial data and conduct secure transactions.
- Long-Term Relationship Damage: Customers who have faced financial losses or inconvenience due to the system failure may start considering moving their accounts to other banks that they perceive as more reliable. This could result in a long-term loss of customer loyalty and revenue for the bank.
- Inconvenience: Customers could not access their funds, purchase, or perform other financial activities during the system outage. While this might not result in direct financial losses, it still causes inconvenience and frustration. For example, the inability to use ATMs and card readers means customers cannot access their money quickly. This creates a significant inconvenience, especially for urgent needs.
- Time and Effort: Customers who encounter failed transactions might need to spend time and effort contacting customer support, visiting the bank's physical branches, or engaging in other activities to resolve issues and recover their funds.
- Transaction Delays: Customers expecting their transactions to be processed promptly would face delays and disruptions in accessing their funds. This could impact their ability to make essential payments or purchases.
- Customer Support Overload: The increased number of calls from frustrated customers overwhelms customer support teams, potentially leading to wait times and reduced service quality.

3.2. Company Loss

Among the effects of data loss similar to the customer, the following can be mentioned (Hannabuss, 2016; Karmakar et al., 2022; Peppers & Rogers, 2017; Wronka, 2023):

- Perceived Reliability: The software company's reputation for providing reliable and secure banking solutions is severely damaged. The incident highlights a significant flaw in their system's design or maintenance, causing clients and prospects to question the company's overall competence.
- Loss of Clients and Contracts: Existing clients might consider switching to other software providers they perceive as more dependable. Prospective clients could be dissuaded from choosing the software company for their projects, leading to lost revenue and growth opportunities.

- Legal and Financial Implications: The software company might face legal actions and financial penalties from the bank due to the losses incurred. They could be required to compensate the bank for financial damages caused by the system failure.
- Operational Disruption: The incident might require the software company to allocate significant resources to diagnose and fix the issue. This disruption could impact ongoing projects and divert attention from other vital tasks.
- Negative Publicity: News of the incident might spread through the industry, affecting the software company's reputation beyond just the immediate client. Negative word-of-mouth and bad publicity can linger for a long time, affecting their ability to attract new clients.
- Business Loss: Existing clients may lose confidence in the software company's ability to provide dependable solutions. This could lead to client churn, where clients switch to competitors, resulting in a loss of revenue and long-term business relationships.
- Client Retention Challenges: Even if the issue is resolved, some clients might still remember and associate the incident with the software company's brand. This could make it harder for the software company to retain and regain clients' trust.
- Future Business Opportunities: Prospective clients might be discouraged from partnering with the software company, fearing similar issues. Future business opportunities could impact the company's ability to secure new contracts and expand its client base.

4. SOLUTIONS FOR REAL CASES

This section is dedicated to exploring what applied solutions can be considered to overcome the underlying challenges. As a typical real-world use- case, we introduce a circumstance where data loss within a software company's banking solutions unit led to severe consequences. Within this study, the loss of sensitive data in the banking solutions unit, where there was a problem with the switching system and database, has led to the loss of bank transaction information. This has caused severe dissatisfaction for thousands of customers. In addition, the contract they have with the bank has caused financial and credit losses. In other words, the transaction switch led to the failure of accepting and issuing transactions and did not provide any response. As a result, the number of calls from switch customers, especially the interbank information transfer network, regarding serious transaction problems, had increased, and bank ATMs and POS were out of order. The stages of the crisis involving the loss of sensitive information and the approach to dealing with it in the banking case study are summarized in Fig. 2.

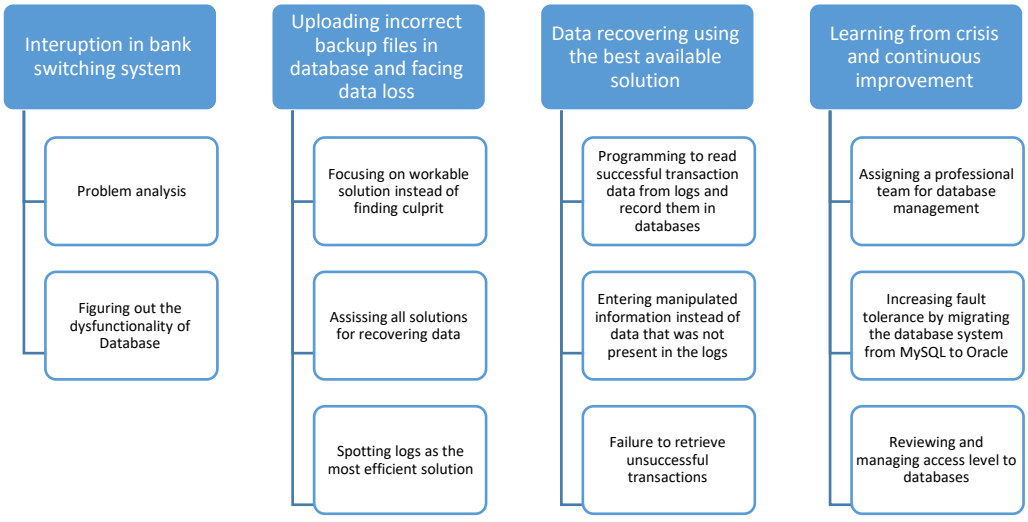

Fig. 2. Reviewing the crisis associated with the case study

Notably, to comprehensively analyze this incident, a structured methodology was employed, involving interviews with senior employees directly involved in handling the data loss event. Insights gained from these interviews provided valuable perspectives on the root causes, challenges faced, and the subsequent solutions implemented in real-world cases. The methodology adopted, specifically the interviewing of key personnel, serves as a methodological approach to studying and understanding the intricacies of the data loss incident.

As a result of these interviews, the paper outlines the available solutions, their side effects, essential indicators, prioritization of solutions, and the fitting of the proper solution to the problem and underlying conditions. The situation we have described is a critical incident in software engineering and financial services. Handling such incidents requires a systematic approach to mitigate the impact on customers, financial losses, and reputation.

4.1. Incident Response

Immediately respond to the incident to minimize further damage. This involves identifying the root cause of the issue, containing the incident, and notifying the relevant stakeholders, including customers, regulatory bodies, and the affected bank.

4.2. Root Cause Analysis

Identify the exact cause of the failure in the switching system and database. It could be due to software bugs, hardware failures, misconfigurations, or security breaches. This step is crucial to prevent the issue from recurring in the future.

4.3. Impact Assessment

Evaluate the extent of the damage caused by the incident. This includes quantifying financial losses, assessing the number of affected customers, understanding the reputational damage, and estimating the time required to recover.

4.4. Applied remedies

To resolve the crisis, the following applied remedies should be considered.

4.4.1. Immediate Fix

Deploy a temporary fix to restore the switching system and database functionality. This might involve restarting services, rolling back to a previous version, or applying a patch.

4.4.2. Data Recovery

If data loss has occurred, attempt to recover as much data as possible. Regular data backups and redundancy strategies can assist in this process.

4.4.3. Communication

Communicate transparently with affected customers, explaining the incident, its impact, and the steps being taken to resolve it. Rebuilding trust is essential.

4.4.4. Performance Improvements

Investigate ways to improve the system's performance to prevent similar incidents in the future. This could involve optimizing code, upgrading hardware, or rearchitecting critical components.

4.4.5. Security Enhancements

Assess the security posture of the system to prevent future breaches. Implement security best practices, conduct vulnerability assessments, and consider penetration testing.

4.5. Side Effects

Each solution can have its side effects:

- Immediate Fix and its Limitations (Immediate Fix which could be a temporary solution and might not address the root cause, leading to future incidents)
- Data Recovery Challenges and Disruptions (Data Recovery which might not recover all data, and the recovery process itself could cause system disruptions)
- Communication and Trust in Incident Response (Communication which May not fully restore customer trust, primarily if not handled transparently and promptly)
- Implementing Performance Improvements (Performance Improvements which could require substantial resources and time to implement)
- Balancing Security Enhancements and Development (Security Enhancements that could slow down development and require changes to existing processes)

4.6. Important Indicators

Key indicators to monitor during the incident response and recovery process include:

- Time to Resolution (how quickly the issue is resolved)
- Customer Satisfaction (feedback from affected customers)
- System Uptime (the time the system is operational after the incident)
- Financial Impact (direct and indirect costs incurred due to the incident)
- Regulatory Compliance (adherence to data protection and financial regulations)

4.7. Prioritization

Prioritize solutions based on their potential impact, feasibility, and urgency:

- Immediate Fix (to restore services)
- Data Recovery (to minimize data loss)
- Communication (to manage customer expectations)
- Security Enhancements (to prevent future incidents)
- Performance Improvements (to ensure stability)

4.8. A proper Solution

The proper solution depends on thoroughly analyzing the incident's root cause and the organization's context. Generally, a combination of immediate fixes, data recovery, improved communication, security enhancements, and performance improvements would be needed to address the incident holistically.

Remember that a multidisciplinary approach involving software engineers, database administrators, security experts, customer service representatives, and management is crucial for effective incident response. Learning from this incident, the organization should also invest in building a more robust incident response plan, improving system monitoring, and implementing preventive measures to minimize the likelihood of similar incidents. The proposed prescription for coping with a crisis is also enumerated in Fig. 3.

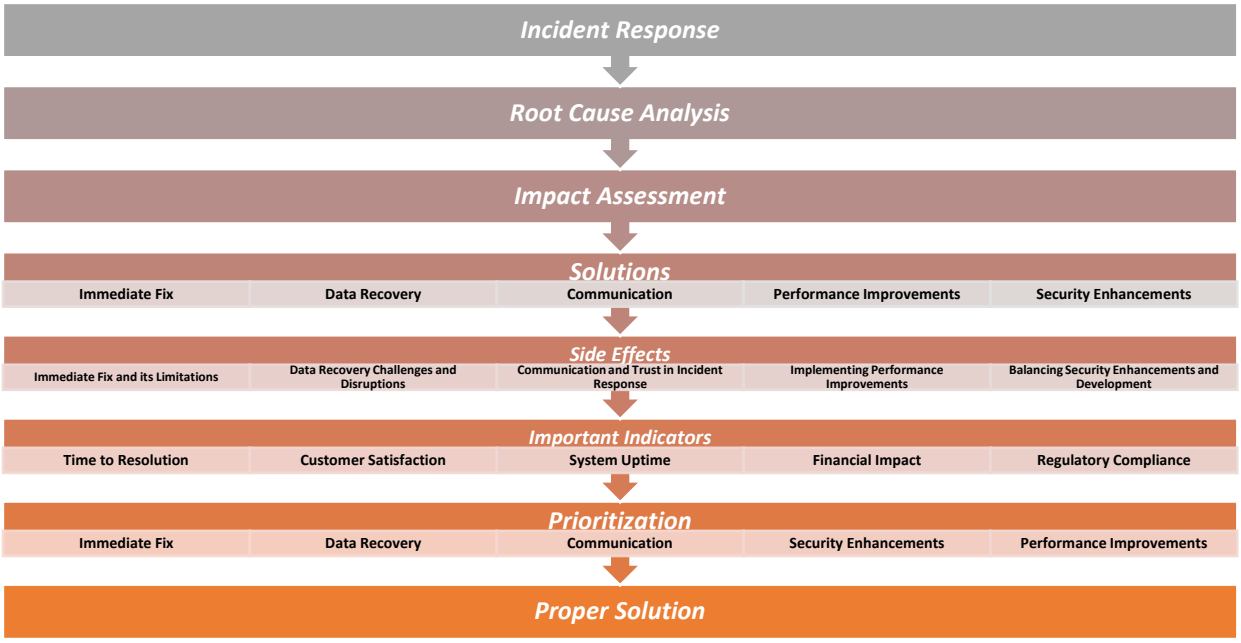

Fig. 3. Steps for mitigating data loss consequences in a critical incident (real-world case)

5. CONCLUSION

In conclusion, data loss poses a significant challenge for organizations utilizing information systems, particularly those with sensitive financial records and customer information. While identifying the causes and vulnerabilities behind data loss incidents is crucial for system improvement, the immediate and secure recovery of lost data is paramount for technical teams. This urgency is especially evident for entities handling sensitive data, as failure to respond appropriately can result in substantial disasters. Within software engineering, data loss involves the unintended removal or destruction of data within a system or database. For software companies with extensive customer databases, such loss can be severe, impacting customer trust, financial records, and operational stability. Recovering lost data aims to restore data integrity and availability, and various methods such as backups, redundancy measures, and replication techniques exist to achieve this. Preventing data loss requires a multifaceted approach. Robust infrastructure, regular maintenance, data security measures, and employee training are vital components. By investing in reliable hardware and software, conducting routine maintenance and testing, implementing access controls and encryption, and educating employees on best practices, software companies can significantly reduce the risk of data loss. The paper also emphasizes the significance of on-the-spot decision-making during crises and reflection on the causes of problems. Additionally, allocating specialized teams for database management, utilizing up-to-date technology, and enforcing proper access controls can contribute to preventing future data loss incidents.

"Focusing on creative solutions" emerges as a guiding principle in critical moments. This approach not only aids in navigating challenges but also directs efforts toward continuous improvement and a more secure future. By embracing this mindset and implementing comprehensive strategies, software companies can safeguard their databases and mitigate the potentially catastrophic consequences of data loss incidents.

REFERENCES

Arogundade, O. R. (2023). Network Security Concepts, Dangers, and Defense Best Practical. Computer Engineering and Intelligent Systems, 14(2).

'De Mesquita, J. M. C., Shin, H., Urdan, A. T., & Pimenta, M. T. C. (2023). Measuring the intention-behavior gap in service failure and recovery: the moderating roles of failure severity and service recovery satisfaction. *European Journal of Marketing*, *57*(7). https://doi.org/10.1108/EJM-03-2022-0235

Ghelani, D., Kian Hua, T., Kumar, S., & Koduru, R. (2022). Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. *American Journal of Computer Science and Technology*, *x*, *No. x*(X).

Hannabuss, S. (2016). The Complete Guide to Business Risk Management (3rd edition). *Reference Reviews*, *30*(5). https://doi.org/10.1108/rr-01-2016-0026

Karmakar, A., Raghuthaman, A., Kote, O. S., & Jayapandian, N. (2022). Cloud Computing Application: Research Challenges and Opportunity. *International Conference on Sustainable Computing and Data Communication Systems, ICSCDS 2022 - Proceedings*. https://doi.org/10.1109/ICSCDS53736.2022.9760887

Khan, A. W., Zaib, S., Khan, F., Tarimer, I., Seo, J. T., & Shin, J. (2022). Analyzing and Evaluating Critical Cyber Security Challenges Faced by Vendor Organizations in Software Development: SLR Based Approach. In *IEEE Access* (Vol. 10). https://doi.org/10.1109/ACCESS.2022.3179822

Khan, S., Gani, A., Wahab, A. W. A., Shiraz, M., & Ahmad, I. (2016). Network forensics: Review, taxonomy, and open challenges. In *Journal of Network and Computer Applications* (Vol. 66). https://doi.org/10.1016/j.jnca.2016.03.005

Khiaonarong, T., Leinonen, H., & Rizaldy, R. (2021). Operational Resilience in Digital Payments: Experiences and Issues. *IMF Working Papers*, *2021*(288). https://doi.org/10.5089/9781616355913.001

Lehto, M. (2022). Cyber-Attacks Against Critical Infrastructure. In *Computational Methods in Applied Sciences* (Vol. 56). https://doi.org/10.1007/978-3-030-91293-2_1

Liu, M., & Yu, L. (2022). Research and Practice on Security Protection and Disaster Recovery Strategy of Oracle Database in Colleges and Universities. *Intelligent Information Management*, *14*(02). https://doi.org/10.4236/iim.2022.142005

Luo, Y., & Zahra, S. A. (2023). Industry 4.0 in international business research. In *Journal of International Business Studies* (Vol. 54, Issue 3). https://doi.org/10.1057/s41267-022-00577-9

Marhaeni, A. A. I. N., Jermsittiparsert, K., Sudarmo, Indrawati, L. R., Prasetyo, A., Fuada, N., Rachmadhani, A., Raharjo, T. W., Wahyudianto, H., Harwijayanti, B. P., Sitorus, J., Fahlevi, M., & Aljuaid, M. (2023). Adoption of the Green Economy through Branchless Rural Credit Banks during the COVID-19 Pandemic in Indonesia. *Sustainability (Switzerland)*, *15*(3). https://doi.org/10.3390/su15032723

Mpofu, F. Y. (2022). Industry 4.0 in Financial Services: Mobile Money Taxes, Revenue Mobilisation, Financial Inclusion, and the Realisation of Sustainable Development Goals (SDGs) in Africa. In *Sustainability (Switzerland)* (Vol. 14, Issue 14). https://doi.org/10.3390/su14148667

OECD. (2021). Artificial Intelligence, Machine Learning and Big Data in Finance: Opportunities, Challenges, and Implications for Policy Makers. *OECD Business and Finance Outlook 2020 : Sustainable and Resilient Finance.*

Peppers, D., & Rogers, M. (2017). Managing Customer Experience and Relationships: A Strategic Framework. *Managing Customer Relationships*.

Ramzan, S., Aqdus, A., Ravi, V., Koundal, D., Amin, R., & Al Ghamdi, M. A. (2022). Healthcare Applications Using Blockchain Technology: Motivations and Challenges. *IEEE Transactions on Engineering Management*. https://doi.org/10.1109/TEM.2022.3189734

Singhal, M. K. (2022). Protecting customer databases to shield business data against ransomware attacks and effective disaster recovery in a hybrid production environment. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3590837.3590927

Tari, Z., Sohrabi, N., Samadi, Y., & Suaboot, J. (2023). Data Exfiltration Threats and Prevention Techniques: Machine Learning and Memory-Based Data Security. In *Data Exfiltration Threats and Prevention Techniques: Machine Learning and Memory-Based Data Security*.

Tripp, J., McKnight, D. H., & Lankton, N. (2022). What most influences consumers' intention to use? different motivation and trust stories for Uber, Airbnb, and taskrabbit. *European Journal of Information Systems*. https://doi.org/10.1080/0960085X.2022.2062469

Vučinić, M., & Luburić, R. (2022). Fintech, Risk-Based Thinking and Cyber Risk. *Journal of Central Banking Theory and Practice*, *11*(2). https://doi.org/10.2478/jcbtp-2022-0012

Wronka, C. (2023). Financial crime in the decentralized finance ecosystem: new challenges for Compliance. *Journal of Financial Crime*, *30*(1). https://doi.org/10.1108/JFC-09-2021-0218