SYMPHONIA
Journal of Theory and Research Output
Volume 1, Issue 1, Januari 2026

The Role Of Forensic Accounting In Addressing Cybercrime And Digital Fraud

Peran Forensik Akuntansi Dalam Menghadapi Kejahatan Siber Dan Kecurangan Digital

Titania Abilla*[1], Lailatusyifa Habibah[2], Gunawan Aji[3]

Universitas Islam Negeri K.H Abdurrahman Wahid, Indonesia [1 2 3]
Corresponding Author: lailatusyifahabibah23@gmail.com

Submitted : 7 Januari 2026	*Revision : 8 Januari 2026*	*Accepted : 9 Januari 2026*

Abstract

This study aims to analyze the role of forensic accounting in detecting and addressing cybercrime and digital fraud in the increasingly complex landscape of technology-based financial systems. The research employs a *library research* method, utilizing data sourced from scholarly articles, books, and official documents relevant to forensic accounting and digital security. An interpretative analysis was conducted to understand the relationship between technological advancement and the application of forensic accounting in digital financial investigations. The results indicate that forensic accounting plays a crucial role in tracing digital evidence, analyzing transactional anomalies, and validating electronic data through *digital forensics*, *fraud analytics*, and *machine learning* techniques. The findings further emphasize the importance of digital auditor competence, technological infrastructure support, and strong data security policies as key factors in preventing and mitigating digital fraud risks.

Keywords: Forensic Accounting; Cybercrime; Digital Fraud; Fraud Analytics; Data Security

Abstrak

Penelitian ini bertujuan untuk menganalisis peran forensik akuntansi dalam mendeteksi dan menangani kejahatan siber serta kecurangan digital yang semakin kompleks di era keuangan berbasis teknologi. Penelitian ini menggunakan metode *library research* dengan sumber data berupa artikel ilmiah, buku, dan dokumen resmi yang relevan dengan topik forensik akuntansi dan keamanan digital. Analisis dilakukan secara interpretatif untuk memahami keterkaitan antara perkembangan teknologi dan penerapan forensik akuntansi dalam konteks investigasi keuangan digital. Hasil penelitian menunjukkan bahwa forensik akuntansi berperan penting dalam penelusuran bukti digital, analisis anomali transaksi, serta validasi data elektronik menggunakan teknik *digital forensics*, *fraud analytics*, dan *machine learning*. Selain itu, temuan juga menegaskan pentingnya kompetensi auditor digital, dukungan infrastruktur teknologi, dan penguatan kebijakan keamanan data sebagai faktor utama dalam mencegah serta mengurangi risiko kecurangan digital.

Kata Kunci: Forensik Akuntansi; Kejahatan Siber; Kecurangan Digital; Fraud Analytics; Keamanan Data

INTRODUCTION

The rapid advancement of digital technology has fundamentally transformed how organizations manage financial transactions and report economic activities. Financial systems that once relied on manual procedures have now shifted to digital platforms offering speed, accuracy, and high efficiency.[1] However, this transformation has also introduced new forms of risk, particularly in the form of cybercrime and digital fraud. Many financial institutions struggle to maintain data integrity and system security, as digitalization often progresses faster than the implementation of adequate internal controls and information security frameworks.[2]

In practice, cases of digital system abuse within the financial sector continue to rise each year. Reports from financial authorities and cybersecurity agencies indicate a significant increase in attacks targeting payment systems, financial applications, and online transaction platforms.rasoo[3] These threats manifest in various forms, including data theft, account hacking, and transaction manipulation. The consequences extend beyond financial losses, damaging institutional reputations and eroding public trust in digital financial services that are expected to ensure safety, transparency, and operational efficiency.

While digital financial systems have brought substantial operational benefits, they have simultaneously expanded the potential for data misuse and transactional fraud. Technology that should enhance transparency can instead be exploited to conceal illicit activities.[4] Many organizations still face challenges in detecting manipulative behavior due to limited digital auditing capabilities and a shortage of professionals skilled in integrating accounting and information technology. This situation underscores the urgent need for adaptive and technology-oriented approaches to address the dynamic and often undetectable nature of digital financial crimes.

Previous research has found that forensic accounting can be highly effective in uncovering fraudulent and unethical financial activities. Other studies highlight that technology-based analytical methods allow more accurate detection of transactional anomalies compared to traditional audits.[5] Additional findings emphasize the importance of integrating digital analytics into organizational monitoring systems. However, most of these studies remain limited to

---

1 Himadri Sikhar Pramanik, Manish Kirtania, and Ashis K. Pani, "Essence of Digital Transformation—Manifestations at Large Financial Institutions from North America," *Future Generation Computer Systems* 95 (June 2019): 323–43, https://doi.org/10.1016/j.future.2018.12.003.

2 Shuang Wang et al., "Data Privacy and Cybersecurity Challenges in the Digital Transformation of the Banking Sector," *Computers & Security* 147 (December 2024): 104051, https://doi.org/10.1016/j.cose.2024.104051.

3 Waqas Ahmed et al., "Security in Next Generation Mobile Payment Systems: A Comprehensive Survey," *IEEE Access* 9 (2021): 115932–50, https://doi.org/10.1109/ACCESS.2021.3105450.

4 Ioannis Mademlis et al., "The Invisible Arms Race: Digital Trends in Illicit Goods Trafficking and AI-Enabled Responses," *IEEE Transactions on Technology and Society* 6, no. 2 (June 2025): 181–99, https://doi.org/10.1109/TTS.2024.3514683.

5 Nitin Singh et al., "Data-driven Auditing: A Predictive Modeling Approach to Fraud Detection and Classification," *Journal of Corporate Accounting & Finance* 30, no. 3 (July 8, 2019): 64–82, https://doi.org/10.1002/jcaf.22389.

conventional financial fraud and have yet to explore the comprehensive application of forensic accounting in addressing cybercrime and digital fraud within modern financial environments.[6]

In response to these developments, this study aims to analyze the role of forensic accounting in detecting, preventing, and managing cybercrime and digital fraud in the digital financial era. The focus is placed on how technology-driven forensic accounting techniques and digital data analysis can enhance internal control systems and strengthen organizational governance. Through a critical interpretative approach based on secondary data, this research seeks to contribute both theoretically and practically to the understanding of digital financial risk management while promoting transparency, accountability, and trust in technology-based financial systems.

Method

This study employs a library research approach, which focuses on collecting and reviewing data from various written and published sources.[7] This method was chosen because the topic of forensic accounting, cybercrime, and digital fraud continues to evolve conceptually and requires an in-depth understanding of existing literature. The data were gathered from credible academic resources, including national and international journal articles, scholarly books, research reports, and relevant official publications. Each source was selected based on its reliability, recency, and relevance to the research theme, ensuring that the resulting analysis maintains academic validity and theoretical depth.

The collected data were analyzed using an interpretative approach, emphasizing critical interpretation of the literature to identify patterns, relationships, and meanings that address the research objectives. This analysis goes beyond describing theories; it also explores how forensic accounting is applied in detecting and responding to cybercrime and digital fraud. Each finding is interpreted in light of technological, legal, and organizational governance aspects. Through this interpretative framework, the library research method enables a comprehensive and contextual understanding of the evolving role of forensic accounting in the digital financial era.

RESULTS AND DISCUSSION

Cybercrime and Digital Fraud in Digital Financial Systems

The development of digital financial systems has greatly enhanced efficiency in managing transactions and financial records across both public and private sectors. Technology enables payment, reporting, and monitoring processes to be carried out quickly and accurately through online networks. However, this advancement also creates new vulnerabilities that can be exploited by irresponsible actors. Financial activities connected to digital platforms have become easy targets for cybercriminals who take advantage of weak security systems, user negligence, and insufficient digital oversight to commit fraud, steal data, or manipulate transactions without leaving physical traces.[8]

---

6 Mario Beluri et al., "Exploration of the Dynamics of Buy and Sale of Social Media Accounts," in *Proceedings of the 2025 ACM Internet Measurement Conference* (New York, NY, USA: ACM, 2025), 32–47, https://doi.org/10.1145/3730567.3732927.

7 Mestika Zed, *Metode Penelitian Kepustakaan* (Yayasan Pustaka Obor Indonesia, 2008).

8 Anastasija Despotović, Ana Parmaković, and Marija Miljković, "Cybercrime and Cyber Security in Fintech," 2023, 255–72, https://doi.org/10.1007/978-3-031-23269-5_15.

Cybercrime in digital financial systems generally involves illegal activities that use computers, networks, or digital devices to gain personal or financial benefit.[9] Such crimes may include hacking into financial accounts, taking control of payment systems, or spreading malware capable of stealing sensitive information. In many cases, perpetrators use phishing techniques to trick users into revealing private information such as passwords or account numbers. These attacks not only cause financial losses but also undermine public trust in financial institutions that become victims of cyberattacks.

Apart from direct system breaches, cybercrime often occurs through the manipulation of transactional data. Perpetrators may alter electronic records, falsify payment proofs, or delete data that could expose suspicious activity.[10] Technology, which is intended to improve efficiency, is instead used to conceal illegal actions. This kind of data manipulation is difficult to detect if organizations lack real-time monitoring systems or effective digital audit procedures. In financial institutions, such fraudulent acts can distort financial statements and threaten the overall stability of operations.

Digital fraud differs significantly from traditional fraud.[11] While conventional fraud is usually committed directly by individuals within an organization, digital fraud often operates automatically and may involve multiple actors across countries. Its methods may include identity theft, automated bot-driven fake transactions, or falsified financial data generated using artificial intelligence. The complexity of technology makes investigating these crimes more challenging, as the evidence exists in digital form and can easily be deleted or modified within seconds.

The transformation of financial operations through digitalization has also introduced new risks that many organizations do not yet fully understand. Dependence on cloud-based systems and interconnected devices increases the potential for sensitive data leaks.[12] Furthermore, many institutions still lack strong internal policies regulating data access. These gaps are often exploited by insiders with system privileges who misuse their authority. This shows that digital fraud and cybercrime are not always external threats; they can also originate from within organizations by individuals familiar with system structures and processes.

The human factor remains a crucial element in the occurrence of cybercrime and digital fraud. Many incidents arise not from weak technology but from poor awareness among users about data security. Simple practices such as using weak passwords, sharing personal information on social media, or ignoring system updates create openings for attackers.[13] Therefore, beyond investing in digital infrastructure, financial institutions must also cultivate a culture of cybersecurity among employees and users to reduce the likelihood of breaches and misuse.

---

9 Norman Mugarura and Emma Ssali, "Intricacies of Anti-Money Laundering and Cyber-Crimes Regulation in a Fluid Global System," *Journal of Money Laundering Control* 24, no. 1 (May 25, 2021): 10–28, https://doi.org/10.1108/JMLC-11-2019-0092.

10 Michail G. Rachavelias, "Online Financial Crimes and Fraud Committed with Electronic Means of Payment—a General Approach and Case Studies in Greece," *ERA Forum* 19, no. 3 (March 24, 2019): 339–55, https://doi.org/10.1007/s12027-018-0519-2.

11 Cassandra Cross, "Is Online Fraud Just Fraud? Examining the Efficacy of the Digital Divide," *Journal of Criminological Research, Policy and Practice* 5, no. 2 (June 10, 2019): 120–31, https://doi.org/10.1108/JCRPP-01-2019-0008.

12 Nivedita Singh, Rajkumar Buyya, and Hyoungshick Kim, "Securing Cloud-Based Internet of Things: Challenges and Mitigations," *Sensors* 25, no. 1 (December 26, 2024): 79, https://doi.org/10.3390/s25010079.

13 M. Yıldırım and I. Mackie, "Encouraging Users to Improve Password Security and Memorability," *International Journal of Information Security* 18, no. 6 (December 11, 2019): 741–59, https://doi.org/10.1007/s10207-019-00429-y.

The impact of cybercrime and digital fraud on financial systems is extensive. Financial loss is only one of the many consequences organizations face.[14] More importantly, such incidents can damage institutional reputation, reduce public confidence, and disrupt economic stability. At a broader level, the growing prevalence of digital fraud poses regulatory challenges for policymakers in updating data protection and digital governance frameworks. This phenomenon highlights that the modern financial world faces not only technical risks but also ethical, legal, and trust-related challenges in maintaining the integrity of digital finance.

The Role of Forensic Accounting in Detecting Cybercrime and Digital Fraud

Forensic accounting plays a crucial role in detecting and investigating both cybercrime and digital fraud within modern financial systems.[15] These two phenomena are closely related, as they both exploit technology to gain unauthorized financial advantage. Unlike conventional audits, which focus on financial compliance, forensic accounting involves a deeper investigation of digital evidence, transactional patterns, and potential system manipulation. In this context, forensic accountants act as investigators who bridge the disciplines of finance, technology, and law, ensuring that digital financial integrity is maintained even in complex technological environments.

Cybercrime typically involves hacking financial systems, stealing data, or gaining illegal control over digital networks. Meanwhile, digital fraud focuses more on manipulating transactions and falsifying financial information within technology-based systems. Forensic accountants must analyze both aspects simultaneously since each leaves different yet interconnected digital traces.[16] Therefore, their ability to identify activity patterns, track user behavior, and verify data authenticity becomes the foundation of effective forensic work in today's digital landscape, where financial evidence is mostly virtual and easily altered.

Table 1. Relationship between Cybercrime and Digital Fraud with the Role of Forensic Accounting

Crime Category	Type of Illegal Activity	Example Case	Role of Forensic Accounting
Cybercrime	Financial system hacking	Unauthorized access to bank servers	Analyze system logs and trace IP origins
Cybercrime	Financial data theft	Extraction of customer records	Audit digital evidence and validate data sources
Digital Fraud	Transaction manipulation	Altering electronic transaction values	Reconstruct data and verify record integrity

[14] Jack Nicholls, Aditya Kuppa, and Nhien-An Le-Khac, "Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape," *IEEE Access* 9 (2021): 163965–86, https://doi.org/10.1109/ACCESS.2021.3134076.

[15] Baljinder Kaur, Kiran Sood, and Simon Grima, "A Systematic Review on Forensic Accounting and Its Contribution towards Fraud Detection and Prevention," *Journal of Financial Regulation and Compliance* 31, no. 1 (January 9, 2023): 60–95, https://doi.org/10.1108/JFRC-02-2022-0015.

[16] Abdallah Kalaf AL-Raggad and Mishael Al-Raggad, "Analyzing Trends: A Bibliometric Study of Administrative Law and Forensic Accounting in the Digital Age," *Heliyon* 10, no. 18 (September 2024): e37462, https://doi.org/10.1016/j.heliyon.2024.e37462.

Digital Fraud	Fabrication of financial reports	Generating fake statements via automation	Apply *fraud analytics* and *AI-based auditing*
Hybrid	Digital evidence deletion	Removing logs to conceal illegal actions	Perform data recovery and document *chain of custody*
Hybrid	Email-based fraud (phishing)	Stealing user login credentials	Analyze digital communications and verify authenticity

Source: author

In practice, forensic accountants employ digital forensics techniques to trace the origin of illegal activity. They analyze user logs, metadata, and suspicious transaction records to determine how breaches occurred. Through these analyses, they can identify who accessed the system, when the intrusion happened, and what impact it had on financial data. In cases of digital fraud, forensic accountants conduct data tracing to reveal inconsistencies between authentic and manipulated records. As shown in *Table 1*, each form of cyber or digital crime requires a specific forensic approach to ensure accuracy and legal reliability in investigation outcomes.

Beyond tracing evidence, forensic accounting also emphasizes transactional pattern analysis. By applying *fraud analytics* and *machine learning*, forensic accountants can detect unusual behaviors such as duplicate transfers, repetitive microtransactions, or cross-account activities that deviate from a user's normal financial profile.[17] This data-driven approach is far more effective than manual auditing in uncovering hidden fraud. Using statistical modeling and machine learning, forensic professionals can separate normal from suspicious behavior and then verify irregularities through detailed digital examination, strengthening detection accuracy and timeliness.

Another vital responsibility involves verification and validation of digital evidence. In both cybercrime and digital fraud cases, data can be easily deleted, modified, or fabricated. Forensic accountants ensure that every piece of evidence collected maintains authenticity and legal integrity.[18] This process includes creating forensic copies, recording *hash values*, and documenting the *chain of custody*. Such measures guarantee that digital evidence remains admissible in court and can withstand legal scrutiny, thereby reinforcing the credibility of forensic accounting within digital financial investigations.

Forensic accounting is not only reactive but also proactive in preventing digital misconduct.[19] Professionals in this field help organizations evaluate system vulnerabilities, enhance internal controls, and develop early detection mechanisms for potential breaches. Preventive steps may include strengthening user authentication, establishing access hierarchies, and implementing automated monitoring for every transaction. Through these actions, forensic accounting serves

[17] Adetunji Paul Adejumo and Chinonso Peter Ogburie, "Forensic Accounting in Financial Fraud Detection: Trends and Challenges," *International Journal of Science and Research Archive* 14, no. 3 (March 30, 2025): 1219–32, https://doi.org/10.30574/ijsra.2025.14.3.0815.

[18] Bryan Howieson, "What Is the 'Good' Forensic Accountant? A Virtue Ethics Perspective," *Pacific Accounting Review* 30, no. 2 (April 3, 2018): 155–67, https://doi.org/10.1108/PAR-01-2017-0005.

[19] Omoize Fatimetu Dako et al., "Forensic Accounting Frameworks Addressing Fraud Prevention in Emerging Markets through Advanced Investigative Auditing Techniques," *Journal of Frontiers in Multidisciplinary Research* 1, no. 2 (2020): 46–63, https://doi.org/10.54660/.JFMR.2020.1.2.46-63.

not merely as an investigative tool after an incident occurs but also as a preventive framework for building safer and more transparent digital financial systems.

Forensic accounting can contributes to human capacity building and digital law enforcement. Forensic accountants often serve as *expert witnesses* in court, translating technical findings into clear legal arguments for judges and investigators.[20] They also provide training to financial staff to recognize early indicators of digital fraud. Educational initiatives like these are essential since many breaches stem from human negligence. With stronger awareness and knowledge of data protection, organizations can enhance digital resilience while maintaining public trust in technology-based financial operations.

CONCLUSION

This study demonstrates that forensic accounting plays a strategic role in addressing the growing complexity of cybercrime and digital fraud within technology-driven financial systems. The findings highlight that the integrated use of *digital forensics*, *fraud analytics*, and *machine learning* significantly enhances the effectiveness of detection, tracing, and verification of digital financial misconduct. Forensic accounting not only serves to identify irregularities but also ensures the authenticity of electronic evidence through reliable verification and validation processes. Furthermore, the study reveals that the success of forensic accounting depends greatly on the readiness of human resources, the availability of technological infrastructure, and the strength of data security policies within financial organizations.

Based on these findings, it is recommended that financial institutions, public agencies, and academic institutions strengthen their forensic accounting capabilities through digital competence development and technology-based internal control systems. Continuous training for auditors, implementation of measurable cybersecurity policies, and investment in forensic analytical tools are essential steps to minimize digital fraud risks. Academically, future research should explore the integration of forensic accounting with artificial intelligence and *blockchain* technologies to further improve financial oversight efficiency. Consequently, forensic accounting is expected to serve as a foundational pillar for building a transparent, secure, and trustworthy digital financial ecosystem.

BIBLIOGRAPHY

Adejumo, Adetunji Paul, and Chinonso Peter Ogburie. "Forensic Accounting in Financial Fraud Detection: Trends and Challenges." *International Journal of Science and Research Archive* 14, no. 3 (March 30, 2025): 1219–32. https://doi.org/10.30574/ijsra.2025.14.3.0815.

Ahmed, Waqas, Aamir Rasool, Abdul Rehman Javed, Neeraj Kumar, Thippa Reddy Gadekallu, Zunera Jalil, and Natalia Kryvinska. "Security in Next Generation Mobile Payment Systems: A Comprehensive Survey." *IEEE Access* 9 (2021): 115932–50. https://doi.org/10.1109/ACCESS.2021.3105450.

AL-Raggad, Abdallah Kalaf, and Mishael Al-Raggad. "Analyzing Trends: A Bibliometric Study of Administrative Law and Forensic Accounting in the Digital Age." *Heliyon* 10, no. 18 (September 2024): e37462. https://doi.org/10.1016/j.heliyon.2024.e37462.

Beluri, Mario, Bhupendra Acharya, Soheil Khodayari, Giada Stivala, Giancarlo Pellegrino, and Thorsten Holz. "Exploration of the Dynamics of Buy and Sale of Social Media Accounts." In *Proceedings of the 2025 ACM Internet Measurement Conference*, 32–47. New York, NY, USA:

[20] Nicole Donahoo, "Accounting Knowledge on Trial: Forensic Accountant Communication in Litigation," 2024, https://doi.org/10.2139/ssrn.4898021.

ACM, 2025. https://doi.org/10.1145/3730567.3732927.

Cross, Cassandra. "Is Online Fraud Just Fraud? Examining the Efficacy of the Digital Divide." *Journal of Criminological Research, Policy and Practice* 5, no. 2 (June 10, 2019): 120–31. https://doi.org/10.1108/JCRPP-01-2019-0008.

Dako, Omoize Fatimetu, Temilola Aderonke Onalaja, Priscilla Samuel Nwachukwu, Folake Ajoke Bankole, and Tewogbade Lateefat. "Forensic Accounting Frameworks Addressing Fraud Prevention in Emerging Markets through Advanced Investigative Auditing Techniques." *Journal of Frontiers in Multidisciplinary Research* 1, no. 2 (2020): 46–63. https://doi.org/10.54660/.JFMR.2020.1.2.46-63.

Despotović, Anastasija, Ana Parmaković, and Marija Miljković. "Cybercrime and Cyber Security in Fintech," 255–72, 2023. https://doi.org/10.1007/978-3-031-23269-5_15.

Donahoo, Nicole. "Accounting Knowledge on Trial: Forensic Accountant Communication in Litigation," 2024. https://doi.org/10.2139/ssrn.4898021.

Howieson, Bryan. "What Is the 'Good' Forensic Accountant? A Virtue Ethics Perspective." *Pacific Accounting Review* 30, no. 2 (April 3, 2018): 155–67. https://doi.org/10.1108/PAR-01-2017-0005.

Kaur, Baljinder, Kiran Sood, and Simon Grima. "A Systematic Review on Forensic Accounting and Its Contribution towards Fraud Detection and Prevention." *Journal of Financial Regulation and Compliance* 31, no. 1 (January 9, 2023): 60–95. https://doi.org/10.1108/JFRC-02-2022-0015.

Mademlis, Ioannis, Marina Mancuso, Caterina Paternoster, Spyridon Evangelatos, Emma Finlay, Joshua Hughes, Panagiotis Radoglou-Grammatikis, et al. "The Invisible Arms Race: Digital Trends in Illicit Goods Trafficking and AI-Enabled Responses." *IEEE Transactions on Technology and Society* 6, no. 2 (June 2025): 181–99. https://doi.org/10.1109/TTS.2024.3514683.

Mugarura, Norman, and Emma Ssali. "Intricacies of Anti-Money Laundering and Cyber-Crimes Regulation in a Fluid Global System." *Journal of Money Laundering Control* 24, no. 1 (May 25, 2021): 10–28. https://doi.org/10.1108/JMLC-11-2019-0092.

Nicholls, Jack, Aditya Kuppa, and Nhien-An Le-Khac. "Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape." *IEEE Access* 9 (2021): 163965–86. https://doi.org/10.1109/ACCESS.2021.3134076.

Pramanik, Himadri Sikhar, Manish Kirtania, and Ashis K. Pani. "Essence of Digital Transformation—Manifestations at Large Financial Institutions from North America." *Future Generation Computer Systems* 95 (June 2019): 323–43. https://doi.org/10.1016/j.future.2018.12.003.

Rachavelias, Michail G. "Online Financial Crimes and Fraud Committed with Electronic Means of Payment—a General Approach and Case Studies in Greece." *ERA Forum* 19, no. 3 (March 24, 2019): 339–55. https://doi.org/10.1007/s12027-018-0519-2.

Singh, Nitin, Kee-hung Lai, Markus Vejvar, and T. C. Edwin Cheng. "Data-driven Auditing: A Predictive Modeling Approach to Fraud Detection and Classification." *Journal of Corporate Accounting & Finance* 30, no. 3 (July 8, 2019): 64–82. https://doi.org/10.1002/jcaf.22389.

Singh, Nivedita, Rajkumar Buyya, and Hyoungshick Kim. "Securing Cloud-Based Internet of Things: Challenges and Mitigations." *Sensors* 25, no. 1 (December 26, 2024): 79.

https://doi.org/10.3390/s25010079.

Wang, Shuang, Muhammad Asif, Muhammad Farrukh Shahzad, and Muhammad Ashfaq. "Data Privacy and Cybersecurity Challenges in the Digital Transformation of the Banking Sector." *Computers & Security* 147 (December 2024): 104051. https://doi.org/10.1016/j.cose.2024.104051.

Yıldırım, M., and I. Mackie. "Encouraging Users to Improve Password Security and Memorability." *International Journal of Information Security* 18, no. 6 (December 11, 2019): 741–59. https://doi.org/10.1007/s10207-019-00429-y.

Zed, Mestika. *Metode Penelitian Kepustakaan*. Yayasan Pustaka Obor Indonesia, 2008.