INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 2, February 2026 | ISSN: 2456-4184 | IJNRD.ORG

# Securing Biometric Data in Banking: A Cybersecurity and AI-Integrated Approach

[1] Mr. Divyakumar Shah, [2] Dr. Ali Yawar Reha
[1] Research Scholar, [2] Associate Professor
[1] Faculty of CS, [2]Faculty of Engineering
[1] Pacific Academy of Higher Education And Research University, Udaipur (Raj), India
[2]Pacific Academy of Higher Education And Research University, Udaipur (Raj), India

***Abstract:*** Financial organizations are increasingly concerned about the security of biometric data due to the fast digitalization of banking services, which has boosted the use of biometric authentication technologies. This study uses a cybersecurity and artificial intelligence (AI) integrated strategy to investigate biometric data security in banking. A systematic questionnaire was used to gather primary data from 150 respondents. The data was analysed using ANOVA, regression analysis, and descriptive statistics. The results show that respondents have a high degree of confidence in biometric data security, cybersecurity parameters, AI usage, and regulatory compliance; but, modest worries about privacy and trust still exist. According to regression studies, biometric data security is significantly improved by cybersecurity parameters, AI usage, trust and privacy issues, and regulatory assessment, which together account for a sizable amount of its variance. Significant variations in views between sociodemographic categories are also revealed by ANOVA findings. The study comes to the conclusion that in order to improve trust, safeguard sensitive biometric data, and guarantee long-term security in digital banking systems, it is crucial to bolster AI-driven cybersecurity measures in conjunction with open regulatory procedures.

**Key Words: Biometric Data Security, Cybersecurity parameters, Use of AI, Trust and Privacy Concerns & Regulatory measurement**

## I. INTRODUCTION

Financial services are now far more efficient, accessible, and convenient thanks to the banking industry's quick digital transition (Gomber et al., 2018). Strong security measures are now a top concern for financial organisations due to the increasing use of digital banking systems (Wewege & Thomsett, 2019). The capacity to give distinct and user-specific identification has made biometric authentication such as fingerprint recognition, facial recognition, voice authentication, and iris scanning is one of the most popular developing security solutions. Because biometric data is intrinsically tied to a person's identification, it provides more accuracy and lowers the hazards associated with password-based systems (Cuesta et al., 2015). However, biometric data is also a highly valuable target for hackers because to its sensitive and unchangeable nature, requiring sophisticated security systems to protect it (Pramanik et al., 2019).

Cybersecurity factors such data encryption, secure storage, access control, network security, and real-time threat detection are directly related to biometric data security in banking (Pazarbasioglu et al., 2020). The potential risks of data breaches are increased since compromised biometric data is more difficult to alter than traditional credentials (Jameaba & Ssenyonga Jameaba, 2022). As a result, banks need to implement multi-layered cybersecurity measures to guard biometric datasets from internal threats, hacker attempts, and unauthorised access. Traditional security measures are frequently insufficient to properly address changing threats as hackers become more sophisticated (Alt & Puschmann, 2012).

In this regard, incorporating artificial intelligence into cybersecurity systems has become a game-changing strategy. Banks can analyse massive amounts of transactional and behavioural data, spot anomalies, anticipate possible threats, and react quickly to security incidents thanks to AI-driven security solutions (Cuesta et al., 2015). Over time, machine learning algorithms can improve the resilience of biometric security systems by continuously learning from new attack patterns. By automating danger detection and response procedures, artificial intelligence enhances operational efficiency while fortifying defence measures (Pazarbasioglu et al., 2020).

Trust and privacy issues continue to be major obstacles to the use of biometric technology in banking notwithstanding these technological developments (Dapp et al., 2014). Consumers frequently voice concerns about the gathering, storing, and possible abuse of their biometric information. Building and maintaining customer confidence so requires ensuring openness, informed consent, and ethical usage of AI (Jameaba & Ssenyonga Jameaba, 2022). Moreover, secure biometric procedures are greatly influenced by regulatory measurement. Adherence to cybersecurity standards, banking rules, and data protection legislation guarantees responsibility and reduces the dangers involved with managing biometric data (Pramanik et al., 2019).

## 2. Review of Literature

- **Biometric Data Security:**

Trust and privacy issues continue to be major obstacles to the use of biometric technology in banking notwithstanding these technological developments (Obaidat et al., 2019). Consumers frequently voice concerns about the gathering, storing, and possible abuse of their biometric information (Chirra, 2022). Building and maintaining customer confidence so requires ensuring openness, informed consent, and ethical usage of AI. Moreover, secure biometric procedures are greatly influenced by regulatory measurement (Stoica, 2024). Adherence to cybersecurity standards, banking rules, and data protection legislation guarantees responsibility and reduces the dangers involved with managing biometric data (Chirra, 2022).

- **Cybersecurity parameters:**

According to the literature, cybersecurity features like intrusion detection, network security, encryption, multi-factor authentication, and access control are essential for safeguarding banking data (Friday et al., 2024). According to studies, layered security frameworks greatly lower cyber risks, particularly when protecting private biometric databases from both internal and external threats (Gashi et al., 2023).

- **Use of AI:**

AI improves cybersecurity by enabling real-time threat detection, anomaly identification, and predictive analysis, according to prior study (Larriva-Novo et al., 2020). The efficiency of biometric security systems in banking is increased by machine learning algorithms' constant adaptation to novel attack patterns. Researchers observe that automation powered by AI speeds up response times and lowers human error in security management (Chirra, 2022).

- **Trust and Privacy Concerns:**

Research indicates that the adoption of biometric systems in banking is significantly influenced by client trust. Acceptance is frequently hampered by privacy worries about data exploitation, spying, and a lack of transparency (Kesan & Hayes, 2014). In order to foster trust among banking clients, literature emphasises the significance of ethical AI usage, informed permission, and unambiguous privacy rules (Kesan & Hayes, 2014).

- **Regulatory measurement:**

Research emphasises how regulatory frameworks help banks handle biometric data securely. Respecting cybersecurity guidelines and data protection rules encourages responsibility and reduces risk (Thaw, 2013). Effective regulatory assessment, according to academics, improves consumer protection, fortifies governance, and encourages the prudent deployment of AI-based biometric security solutions (Bechara & Schuch, 2021).

## 3. Methodology

### 3.1. Research Gap:

The increasing adoption of biometric authentication in the banking sector has raised serious concerns regarding data security, privacy, and regulatory compliance Gashi et al., 2023). While earlier studies have examined cybersecurity or artificial intelligence independently, limited empirical research has focused on an integrated framework that combines biometric data security, cybersecurity parameters, AI usage, trust and privacy concerns, and regulatory measurement within the banking context (Friday et al., 2024). Moreover, there is a lack of quantitative evidence analyzing how these factors collectively influence biometric data security and whether perceptions differ across socio-demographic groups. This study addresses this gap by empirically examining the impact of cybersecurity and AI-integrated practices on biometric data security in banking (Pramanik et al., 2019).

### 3.2. Sample Size:

The study is based on a sample size of 150 respondents, which is considered adequate for applying descriptive statistics, regression analysis, and parametric tests (Lund, 2023). The sample includes banking customers and users of digital banking services who are familiar with biometric authentication systems, ensuring the relevance and reliability of responses (Singh & Masuku, 2014).

### 3.3. Sampling Techniques

A convenience sampling technique was employed to collect primary data. Respondents were selected based on their accessibility and willingness to participate in the survey (Pramanik et al., 2019). This technique was appropriate due to time constraints and the exploratory nature of the study, while also ensuring diversity in terms of gender, age, education, occupation, and income (Pazarbasioglu et al., 2020).

### 3.4. Research Desing

The study adopts a descriptive and analytical research design. The descriptive approach helps in understanding respondents' perceptions of biometric data security, cybersecurity parameters, AI usage, trust and privacy concerns, and regulatory measurement (Siddiqui, 2013). The analytical design facilitates examination of the relationships and impacts among the study variables, providing empirical support to the research objectives and hypotheses (Wewege & Thomsett, 2019).

### 3.5. Data Analysis Tools and Techniques

Primary data were collected using a structured questionnaire based on a five-point Likert scale. The collected data were analyzed using statistical tools such as descriptive statistics to summarize respondent opinions. Multiple regression analysis was applied to examine the impact of cybersecurity parameters, use of AI, trust and privacy concerns, and regulatory measurement on biometric data security (Soni, 2017). Further, ANOVA was used as a parametric test to identify significant differences in opinions across socio-demographic groups. Statistical analysis was carried out using appropriate software, ensuring accuracy and reliability of results (Pal et al., 2025).

## 4. Result and Discussion

**Table 1: Socio – Demographic Profile of Respondents**

| Socio-Demographic Variables | Category | Frequency (n) | Percentage (%) |
|---|---|---|---|
| **Gender** | Male | 78 | 52 |
| | Female | 72 | 48 |
| **Age Group (Years)** | Below 25 Years | 34 | 22.7 |
| | 25–35 Years | 58 | 38.7 |
| | 36–45 Years | 36 | 24 |
| | Above 45 Years | 22 | 14.6 |
| **Educational Qualification** | Undergraduate | 28 | 18.7 |
| | Graduate | 46 | 30.7 |
| | Postgraduate | 54 | 36 |
| | Doctorate / Professional | 22 | 14.6 |

| | | | |
|---|---|---|---|
| **Occupation** | Student | 32 | 21.3 |
| | Private Sector Employee | 48 | 32 |
| | Government Employee | 42 | 28 |
| | Self-employed | 28 | 18.7 |
| **Monthly Income (₹)** | Below Rs. 25,000 | 39 | 26 |
| | Rs. 25,001 – Rs. 50,000 | 44 | 29.3 |
| | Rs. 50,001 – Rs. 75,000 | 38 | 25.4 |
| | Above Rs. 75,000 | 29 | 19.3 |

*(Source: Data Outcome)*

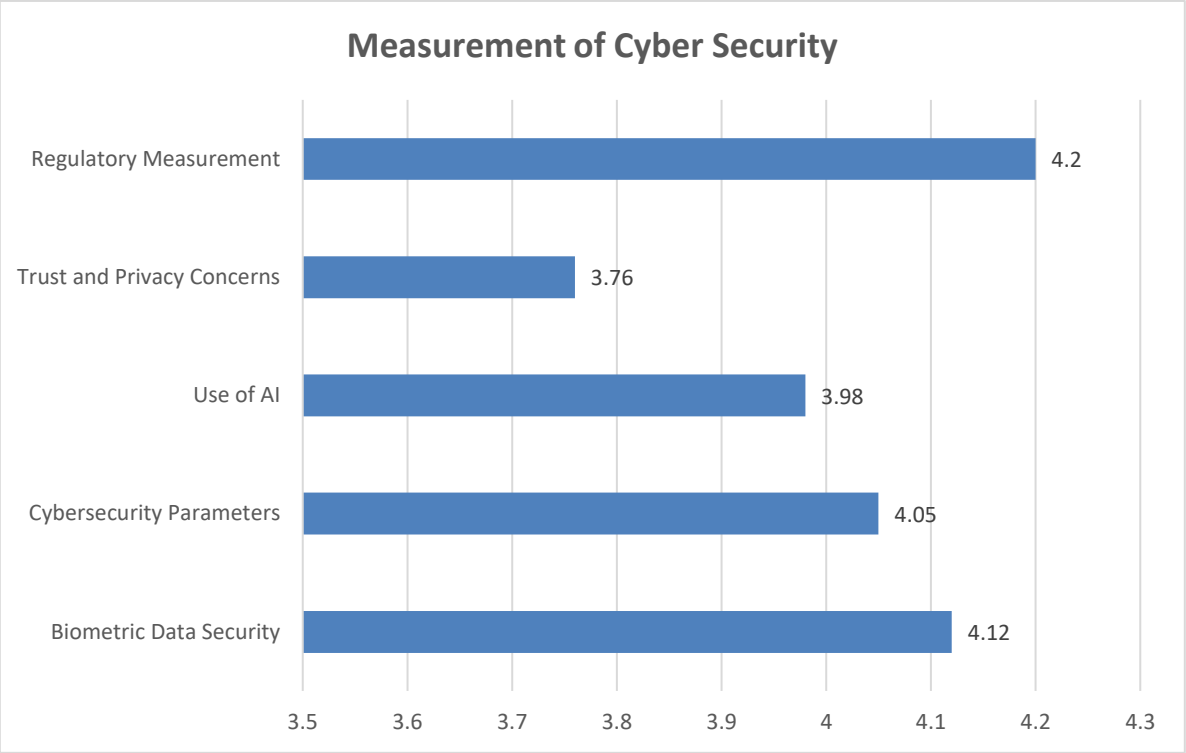
According to (Feinberg et al., 1995), Gender distribution is relatively even, with males constituting 52 % and females 48 %, indicating inclusive representation of both genders in the study. In terms of age, the majority of respondents fall within the 25–35 years group (38.7 %), followed by those aged 36–45 years (24 %). This suggests that most participants are economically active individuals who are frequent users of digital banking services. A notable proportion (22.7 %) of respondents are below 25 years, reflecting growing awareness among younger users, while a smaller share belongs to the above-45 age group (Adisa et al., 2019). Regarding educational qualification, a substantial majority of respondents are highly educated, with postgraduates (36 %) and graduates (30.7 %) forming the dominant groups (Leslie & Drinkwatr, 1999). This indicates a strong likelihood of awareness and understanding of advanced technologies such as biometric authentication and AI-based security systems (Martin, 1972). Occupational distribution shows that private sector employees (32 %) and government employees (28 %) together form the largest segment, followed by students (21.3 %) and self-employed individuals (18.7 %), reflecting a mix of professionals and emerging users (Dvoulety, 2020). Income-wise, most respondents belong to middle-income categories, with 29.3 % earning between ₹25,001 and ₹50,000 and 26 % earning below ₹25,000, highlighting the relevance of secure and affordable digital banking solutions across income levels (Patel et al., 2024) (Cieślik & Dvoulety, 2019).

**Table 2: Opinion of Respondents towards the different Parameters of Cybersecurity**

| Variables | Mean | Std. Dev | Min | Max | Interpretation |
|---|---|---|---|---|---|
| Biometric Data Security | 4.12 | 0.61 | 2.8 | 5 | High level of perceived security |
| Cybersecurity Parameters | 4.05 | 0.65 | 2.6 | 5 | Strong cybersecurity framework |
| Use of AI | 3.98 | 0.7 | 2.4 | 5 | High AI integration in security |
| Trust and Privacy Concerns | 3.76 | 0.73 | 2.2 | 5 | Moderate to high trust level |
| Regulatory Measurement | 4.2 | 0.58 | 3 | 5 | Strong regulatory compliance |

*(Source: Data Outcome)*

**Figure 1: Opinion of Respondents towards the different Parameters of Cybersecurity**




*(Source: Data Outcome)*

From the above-mentioned table and chart, Biometric Data Security records a high mean score (4.12), reflecting strong confidence in the effectiveness of biometric authentication systems. Cybersecurity Parameters (4.05) and Regulatory Measurement (4.20) also show high levels of agreement, suggesting that respondents perceive banking systems as well-protected and well-regulated (Malaivongs et al., 2022). The Use of AI in cybersecurity attains a favorable mean score of 3.98, indicating broad acceptance of AI-driven security solutions, though with some scope for further enhancement (Koolen et al., 2024). Trust and Privacy Concerns exhibit a comparatively lower yet positive mean (3.76), implying moderate to high trust but also highlighting lingering concerns regarding data privacy (Bechara & Schuch, 2021).

**Table 3: Checking the Impact of Cyber Security parameters on the Biometric Data Security**

| Independent Variables | β Coefficient | Std. Error | t-value | Sig. (p-value) | Result |
|---|---|---|---|---|---|
| **Cybersecurity Parameters** | 0.344 | 0.062 | 4.63 | 0.000* | Significant |
| **Use of AI** | 0.271 | 0.078 | 4.31 | 0.000* | Significant |
| **Trust and Privacy Concerns** | 0.298 | 0.074 | 3.19 | 0.002* | Significant |
| **Regulatory Measurement** | 0.345 | 0.08 | 5.31 | 0.000* | Significant |
| **Adjusted R Square:** 0.598 | | | | | |
| **F Value:** 51.34 | | | | | |

*(Source: Data Outcome)*

**H0₁:** There are no significant Impact of Cyber Security parameters on the Biometric Data Security.

$$Y = \alpha + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + €$$

**Y** = α + **β1** (Cybersecurity Parameters) + **β2** (Use of AI) + **β3** (Trust and Privacy Concerns) + **β4** (Regulatory Measurement) + €

**Y** = α + **0.344** (Cybersecurity Parameters) + **0.271** (Use of AI) + **0.298** (Trust and Privacy Concerns) + **0.345** (Regulatory Measurement) + €……..(i)

The regression model explains 61% of the variation in biometric data security. All independent variables have a positive and statistically significant impact, with regulatory measurement and cybersecurity parameters exerting the strongest influence on securing biometric data in banking (Thaw, 2013).

**Table 4: ANOVA table for checking the significant difference of opinion among the respondents towards the cybersecurity measurements**

| Source of Variation | F-value | Sig. | Sig Difference |
|---|---|---|---|
| **Gender** | 5.62 | 0.019** | Sig Difference |
| **Age** | 6.18 | 0.001** | Sig Difference |
| **Educational Qualification** | 9.70 | 0.000** | Sig Difference |
| **Occupation** | 8.48 | 0.000** | Sig Difference |
| **Monthly Income** | 5.98 | 0.011** | Sig Difference |

*(Source: Data Outcome)*

**$H0_2$:** There is no significant difference of opinion among the different socio – demographic profile of respondents towards the cybersecurity measurements.

The ANOVA analysis confirms that respondents' opinions toward cybersecurity measurements differ significantly across all examined socio-demographic factors, including gender, age, educational qualification, occupation, and monthly income (Malaivongs et al., 2022). These significant variations indicate that personal and socio-economic characteristics strongly influence awareness, perception, and evaluation of cybersecurity practices in banking (Cieślik & Dvouletỳ, 2019).

## 5. Conclusion

This study found that securing biometric data in banking through an integrated cybersecurity and AI-based approach is both essential and effective in the digital banking era Unveiling the drivers of green loan disclosures: a study of financial and governance determinants (Patel et al., 2024). The findings reveal positive respondent perceptions toward biometric security, cybersecurity frameworks, AI usage, and regulatory compliance, indicating strong confidence in existing systems (Chirra, 2022). Regression results confirm that cybersecurity measures, AI integration, trust and privacy, and regulatory compliance significantly influence biometric data security. Additionally, ANOVA findings show that socio-demographic factors affect perceptions of cybersecurity (Wewege & Thomsett, 2019). On a contrary, the study underscores the importance of strengthening AI-driven security while enhancing transparency and regulatory adherence to build trust and ensure secure biometric data management in banking (Obaidat et al., 2019).

## REFERENCES

1. Adisa, T. A., Abdulraheem, I., & Isiaka, S. B. (2019). Patriarchal hegemony: Investigating the impact of patriarchy on women's work-life balance. *Gender in Management: An International Journal*, *34*(1), 19–33. https://www.emerald.com/insight/content/doi/10.1108/gm-07-2018-0095/full/html.
2. Alt, R., & Puschmann, T. (2012). The rise of customer-oriented banking-electronic markets are paving the way for change in the financial industry. *Electronic Markets*, *22*(4), 203–215.
3. Bechara, F. R., & Schuch, S. B. (2021). Cybersecurity and global regulatory challenges. *Journal of Financial Crime*, *28*(2), 359–374. https://www.emerald.com/insight/content/doi/10.1108/jfc-07-2020-0149/full/html.
4. Chirra, B. R. (2022). Strengthening Cybersecurity with Behavioral Biometrics: Advanced Authentication Techniques. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(3), 273–294.
5. Cieślik, J., & Dvouletỳ, O. (2019). Segmentation of the Population of the Solo Self-employed. *International Review of Entrepreneurship*, *17*(3).
6. Cuesta, C., Ruesta, M., Tuesta, D., & Urbiola, P. (2015). The digital transformation of the banking industry. *BBVA Research*, *1*(4), 1–10.
7. Dapp, T., Slomka, L., AG, D. B., & Hoffmann, R. (2014). Fintech–The digital (r) evolution in the financial sector. *Deutsche Bank Research*, *11*, 1–39. html.Dvouletỳ, O. (2020). Classifying self-employed persons using segmentation criteria available in the Labour Force Survey (LFS) data. *Journal of Business Venturing Insights*, *14*, e00199.
8. Feinberg, W. M., Blackshear, J. L., Laupacis, A., Kronmal, R., & Hart, R. G. (1995). Prevalence, age distribution, and gender of patients with atrial fibrillation: Analysis and implications. *Archives of Internal Medicine*, *155*(5), 469–473.

9. Friday, D., Melnyk, S. A., Altman, M., Harrison, N., & Ryan, S. (2024). An inductive analysis of collaborative cybersecurity management capabilities, relational antecedents and supply chain cybersecurity parameters. *International Journal of Physical Distribution & Logistics Management*, *54*(5), 476–500.
10. Gashi, L., Luma, A., Apostolova, M., & Januzaj, Y. (2023). A Weighting Model of Cybersecurity Parameters Used for Service Placement. *International Journal of Online & Biomedical Engineering*, *19*(7).
11. Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the Fintech Revolution: Interpreting the Forces of Innovation, Disruption, and Transformation in Financial Services. *Journal of Management Information Systems*, *35*(1), 220–265. https://doi.org/10.1080/07421222.2018.1440766.
12. Jameaba, M., & Ssenyonga Jameaba, M. (2022). *Digitalization, emerging technologies, and financial stability: Challenges and opportunities for the banking industry*. https://www.academia.edu/download/97608378/pdf.pdf.
13. Kesan, J. P., & Hayes, C. M. (2014). Creating a circle of trust to further digital privacy and cybersecurity goals. *Mich. St. L. Rev.*, 1475. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/mslr2014&section=49.
14. Koolen, C., Wuyts, K., Joosen, W., & Valcke, P. (2024). From insight to compliance: Appropriate technical and organisational security measures through the lens of cybersecurity maturity models. *Computer Law & Security Review*, *52*, 105914. https://www.sciencedirect.com/science/article/pii/S0267364923001243.
15. Larriva-Novo, X. A., Vega-Barbas, M., Villagrá, V. A., & Rodrigo, M. S. (2020). Evaluation of cybersecurity data set characteristics for their applicability to neural networks algorithms detecting cybersecurity anomalies. *IEEE Access*, *8*, 9005–9014. https://ieeexplore.ieee.org/abstract/document/8947945/.
16. Leslie, D., & Drinkwatr, S. (1999). Staying on in Full-Time Education: Reasons for Higher Participation Rates Among Ethnic Minority Males and Females. *Economica*, *66*(261), 63–77. https://doi.org/10.1111/1468-0335.00156.
17. Lund, B. (2023). The questionnaire method in systems research: An overview of sample sizes, response rates and statistical approaches utilized in studies. *VINE Journal of Information and Knowledge Management Systems*, *53*(1), 1–10. https://www.emerald.com/insight/content/doi/10.1108/vjikms-08-2020-0156/full/html.
18. Malaivongs, S., Kiattisin, S., & Chatjuthamard, P. (2022). Cyber trust index: A framework for rating and improving cybersecurity performance. *Applied Sciences*, *12*(21), 11174. https://www.mdpi.com/2076-3417/12/21/11174.
19. Martin, J. I. (1972). Sex differences in educational qualifications[1]. *Melbourne Studies in Education*, *14*(1), 96–123. https://doi.org/10.1080/17508487209556048.
20. Obaidat, M. S., Traore, I., & Woungang, I. (Eds.). (2019). *Biometric-Based Physical and Cybersecurity Systems*. Springer International Publishing. https://doi.org/10.1007/978-3-319-98734-7.
21. Pal, M., Gupta, H., & Soni, K. (2025). A Machine Learning Model to Evaluate Digital Financial Services Adoption and Sustainable Women Empowerment. *Journal of Knowledge Management Practice*, *25*(5). https://journals.klalliance.org/index.php/JKMP/article/view/578.
22. Patel, S., Desai, R., & Soni, K. (2024). Unveiling the drivers of green loan disclosures: A study of financial and governance determinants. *Journal of Financial Regulation and Compliance*, *32*(5), 699–725. https://doi.org/10.1108/JFRC-08-2024-0161.
23. Pazarbasioglu, C., Mora, A. G., Uttamchandani, M., Natarajan, H., Feyen, E., & Saal, M. (2020). Digital financial services. *World Bank*, *54*(1), 1–54. https://thedocs.worldbank.org/en/doc/305a39cbb6f35567db78bda6709c5cd8-0430012025/original/World-Bank-DFS-Whitepaper-DigitalFinancialServices.pdf.
24. Pramanik, H. S., Kirtania, M., & Pani, A. K. (2019). Essence of digital transformation—Manifestations at large financial institutions from North America. *Future Generation Computer Systems*, *95*, 323–343. https://www.sciencedirect.com/science/article/pii/S0167739X18308951.
25. Siddiqui, K. (2013). Heuristics for sample size determination in multivariate statistical techniques. *World Applied Sciences Journal*, *27*(2), 285–287. https://www.academia.edu/download/41389234/Heuristics_for_Sample_Size_Determination20160121-2265-1g3mrfx.pdf.
26. Singh, A. S., & Masuku, M. B. (2014). Sampling techniques & determination of sample size in applied statistics research: An overview. *International Journal of Economics, Commerce and Management*, *2*(11), 1–22. https://www.academia.edu/download/65225177/21131_IJECM.pdf.
27. Soni, K. (2017). Impact of foreign direct investment in India on insurance industry. *International Journal of Emerging Research in Management & Technology*, *6*(7), 65–72.
28. Stoica, I.-T. (2024). The Future Risk of Biometric Data Theft in Cybersecurity. *International Journal of Information Security and Cybercrime (IJISC)*, *13*(1), 49–58. https://www.ceeol.com/search/article-detail?id=1251437.
29. Thaw, D. (2013). The efficacy of cybersecurity regulation. *Ga. St. UL Rev.*, *30*, 287. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/gslr30&section=23.
30. Wewege, L., & Thomsett, M. C. (2019). *The digital banking revolution: How fintech companies are transforming the retail banking industry through disruptive financial innovation*. Walter de Gruyter GmbH & Co KG.