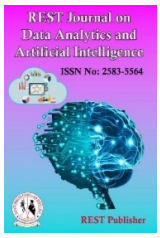
REST Publisher; ISSN No: 2583-5564 (Online)

REST Journal on Data Analytics and Artificial Intelligence

journal homepage: https://restpublisher.com/journals/jdaai/



Optimizing Banking Security: A Comparative Study of Biometric Authentication Methods

Devipriya Mani*, M. Ramachandran, Vidhya Prasanth

REST Labs, Kaveripattinam, Krishnagiri, Tamil Nadu, India.

ARTICLE INFO

Article history:
Received: 30 October 2026
Accepted: 02 November 2026
Available online: 21 November 2026

Keywords:
Fingerprint Recognition
Facial Recognition
Iris Scan
Accuracy (%)
Security Level
User Convenience
Implementation Cost ($)

ABSTRACT

The impact of biometric authentication on banking security Biometric authentication is revolutionizing banking security by offering a highly secure, accurate, and convenient method of user verification. Unlike traditional passwords and PINs, biometrics such as fingerprints, facial recognition, iris scans, and voice recognition are unique to individuals, making fraud and identity theft significantly harder. Research significance: This research on banking security is significant as it addresses critical challenges in financial security, fraud prevention, and user authentication. Methodology: This study employs a mixed-methods approach to analyze the impact of biometric authentication on banking security. Primary data is collected through surveys and interviews with banking professionals and customers to assess their perceptions of biometric security, convenience, and fraud prevention. Secondary data is gathered from academic journals, industry reports, and case studies on biometric authentication. A comparative analysis of different biometric modalities, including fingerprint recognition, facial recognition, and iris scanning, is conducted based on security effectiveness, accuracy, and implementation challenges. Statistical tools are used to evaluate fraud reduction rates, customer adoption, and the cost-effectiveness of biometric security systems. Alternative: Fingerprint Recognition, Facial Recognition, Iris Scan, Voice Recognition, Palm Vein Recognition, Behavioral Biometrics, Retina Scan, Hand Geometry Evaluation preference: Accuracy (%), Security Level, User Convenience, Implementation Cost ($), Processing Speed (ms), Fraud Detection Effectiveness Results: Fingerprint Recognition is getting top of the table and Retina Scan is getting bottom of the table

1. INTRODUCTION

In the digital age, the banking sector is continuously evolving to meet the increasing demands for security, efficiency, and customer convenience. With the rise of cyber threats, such as passwords and PINs have become insufficient in safeguarding sensitive financial data. Biometric authentication has emerged as a transformative technology in banking security, offering a robust and user-friendly alternative to conventional authentication methods [1]. Banking security has evolved significantly over the past few decades. Traditionally, banking transactions were conducted in person, requiring physical verification through signatures or ID cards. As online banking gained popularity, authentication methods such as PINs and passwords became the primary security measures [2]. Several types of biometric authentication are being deployed in the banking sector to strengthen security and streamline customer interactions. Many banking apps and ATMs now allow customers to authenticate transactions using their fingerprints [3]. Banks can streamline operations by reducing the need for manual identity verification, leading to faster transaction processing and improved customer service. Many financial regulatory

*Corresponding author email-id: devipriyarsri2005@gmail.com
DOI: https://doi.org/10.46632/jdaai/5/4/2
Copyright @ 2026 Published by REST Publisher

bodies encourage the adoption of biometric authentication to enhance data protection and fraud prevention measures. While the initial implementation of biometric systems may be costly, banks can save money losses from fraud and eliminating the need for password resets and account recovery services [4]. AI and machine learning integration allow AI-driven biometric systems to perform real-time fraud detection and risk assessment. Block chain technology is being leveraged for biometric data security, ensuring safe storage and management of biometric credentials [5]. However, challenges such as privacy concerns, implementation costs, and cyber security threats must be addressed to maximize the benefits of biometric security in banking. As technology continues to evolve, biometric authentication will play an increasingly crucial role in securing financial transactions and enhancing customer trust in the banking sector [6]. Beyond security, another significant advantage of biometric authentication in banking is its ability to enhance customer experience by providing a seamless and convenient method of authentication. Traditional banking authentication methods often involve remembering complex passwords or carrying physical tokens, which can be cumbersome for customers [7]. This not only improves the overall user experience but also accelerates banking processes by reducing authentication time. Mobile banking apps, ATMs, and digital wallets are increasingly integrating biometric authentication to provide faster and more efficient services. For instance, many banks now allow customers to log into their accounts using fingerprint or facial recognition instead of entering passwords, making digital banking more user-friendly and accessible. [8] In addition to user convenience, biometric authentication significantly strengthens fraud prevention and risk management in banking. Traditional security measures are highly susceptible to breaches, as hackers can steal passwords or intercept authentication codes [9]. For example, facial recognition systems incorporate depth-sensing technology to differentiate between a real face and a photograph, while fingerprint scanners detect blood flow to ensure that the fingerprint belongs to a living individual. Such advanced security features make biometric authentication an effective tool in mitigating fraudulent activities such as account takeovers, identity theft, and unauthorized transactions [10]. Another challenge associated with biometric authentication is the cost of implementation. Deploying biometric security systems requires substantial investment in hardware, software, and infrastructure. High-end biometric scanners, liveness detection technologies, and AI-driven fraud detection mechanisms can be expensive, making it difficult for smaller banks and financial institutions to adopt biometric authentication on a large scale. [11] Moreover, the integration of biometric authentication with existing banking systems requires significant technological upgrades and ongoing maintenance, adding to the overall cost burden [12]. Additionally, biometric authentication is not entirely foolproof and can sometimes produce false positives or false negatives. Factors such as poor lighting conditions, facial changes due to aging, skin conditions affecting fingerprints, and voice distortions can impact the accuracy of biometric authentication [13]. Looking ahead, the future of biometric authentication in banking appears promising, with continuous advancements in technology driving innovation in security and user experience. Emerging trends such as multimodal biometrics, which combine multiple biometric modalities for enhanced security, are gaining popularity in the financial sector [14]. For example, banks are increasingly integrating fingerprint and facial recognition, or voice and behavioral biometrics, to provide multi-layered authentication solutions. Moreover, the rise of artificial intelligence and deep learning is further enhancing the accuracy and efficiency of biometric systems, making them more resilient against security threats. [15] Furthermore, the advent of decentralized identity solutions and block chain-based biometric authentication is expected to revolutionize banking security by providing greater control over personal biometric data [16].

2. MATERIAL AND METHOD

Alternative:

- **Fingerprint Recognition:** One of the most widely used biometric authentication methods, fingerprint recognition identifies individuals based on unique fingerprint patterns. It is fast, reliable, and cost-effective, making it ideal for banking applications.
- **Facial Recognition:** This technology analyzes facial features to verify identity. It offers contactless authentication, improving user convenience. However, its accuracy can be affected by lighting conditions and facial changes.
- **Iris Scan:** Iris recognition uses the unique patterns in the iris to authenticate users. It is highly secure and has low false acceptance rates, but its high implementation cost makes it less common in consumer banking.

- **Voice Recognition:** This method analyzes an individual's voiceprint to verify identity. It enhances remote banking security but may be affected by background noise or voice changes due to illness.
- **Palm Vein Recognition:** This technique scans the vein patterns inside the palm, offering high security and resistance to forgery. However, it requires specialized scanners, increasing deployment costs.
- **Behavioral Biometrics:** This method examines patterns in user behavior, such as keystroke dynamics and mouse movements, to detect anomalies and prevent fraud.
- **Retina Scan:** By analyzing the unique blood vessel pattern in the retina, this method provides high security but is intrusive and expensive.
- **Hand Geometry:** This system measures the shape and size of a person's hand. It is less secure but useful for low-risk banking applications.

Evaluation Parameters:

- **Accuracy (%):** Accuracy measures the biometric system's ability to correctly authenticate users while minimizing false acceptances and rejections. Higher accuracy ensures better security and user experience, making it a crucial factor in banking applications.
- **Security Level:** Security level refers to how resistant a biometric system is to spoofing and fraud attempts. Methods like iris scans and retina recognition offer higher security compared to facial or voice recognition, which can be more vulnerable to deepfake attacks or environmental factors.
- **User Convenience:** A balance between security and ease of use is essential. Fingerprint and facial recognition are highly convenient, offering quick, seamless authentication, while retina scans and palm vein recognition require specialized hardware, making them less user-friendly.
- **Implementation Cost ($):** The cost of deploying biometric systems varies significantly. Fingerprint and facial recognition are cost-effective, whereas iris scans, retina scans, and palm vein recognition involve higher costs due to specialized equipment and complex infrastructure.
- **Processing Speed (ms):** This metric evaluates how quickly a biometric system verifies identity. Faster systems improve customer experience and reduce wait times, which is vital in high-traffic banking environments.
- **Fraud Detection Effectiveness:** The system's ability to detect and prevent fraudulent access is key. Behavioral biometrics and multi-modal authentication methods enhance fraud prevention by analyzing user patterns and detecting anomalies beyond traditional biometric verification.

3. MOORA METHOD

The Multi-Objective Optimization by Ratio Analysis (MOORA) method is a decision-making approach used to evaluate and rank multiple alternatives based on various criteria. It is widely applied in fields like engineering, economics, and security, where multiple factors need to be considered simultaneously.[17] MOORA simplifies complex decision-making by distinguishing between beneficial criteria, which should be maximized (e.g., accuracy, security level, and user convenience in biometric authentication), and non-beneficial criteria, which should be minimized (e.g., cost, processing time, and energy consumption).[18] The process begins with normalization, where different criteria with varying units are converted into a comparable scale. Next, weights are assigned to each criterion based on its importance. The method then calculates an overall score for each alternative by summing the beneficial criteria and subtracting the non-beneficial ones. Finally, alternatives are ranked, with the highest score representing the most optimal choice.[19] In biometric authentication, MOORA helps evaluate technologies like fingerprint recognition, facial recognition, iris scan, and others, ensuring the best balance between security, cost, and efficiency. By systematically assessing multiple factors, MOORA provides a structured, transparent, and effective way to make logical and informed decisions in various industries.[20]

4. RESULT AND DISCUSSION

TABLE 1. The Impact of Biometric Authentication on Banking Security

Biometric Authentication	Accuracy (%)	Security Level	User Convenience	Implementation Cost ($)	Processing Speed (ms)	Fraud Detection Effectiveness
Fingerprint Recognition	98	9	9	300	150	8
Facial Recognition	95	8	9	500	200	7
Iris Scan	99	10	7	1200	300	9
Voice Recognition	92	7	8	750	250	6
Palm Vein Recognition	97	9	6	1600	350	9
Behavioral Biometrics	90	7	9	1230	180	7
Retina Scan	99	10	5	1450	400	10
Hand Geometry	93	8	7	1740	280	7

Table 1 presents the evaluates different biometric authentication techniques for banking security using the MOORA method, considering six parameters: accuracy, security, convenience, cost, processing speed, and fraud detection. Iris and retina scans provide the highest accuracy and security but involve substantial implementation costs and reduced convenience. Fingerprint and palm vein recognition offer a balanced combination of reliability and fraud prevention. Facial recognition and behavioral biometrics ensure greater user convenience with satisfactory performance. However, behavioral biometrics requires higher investment. Voice recognition and hand geometry show moderate effectiveness with slower processing speeds.

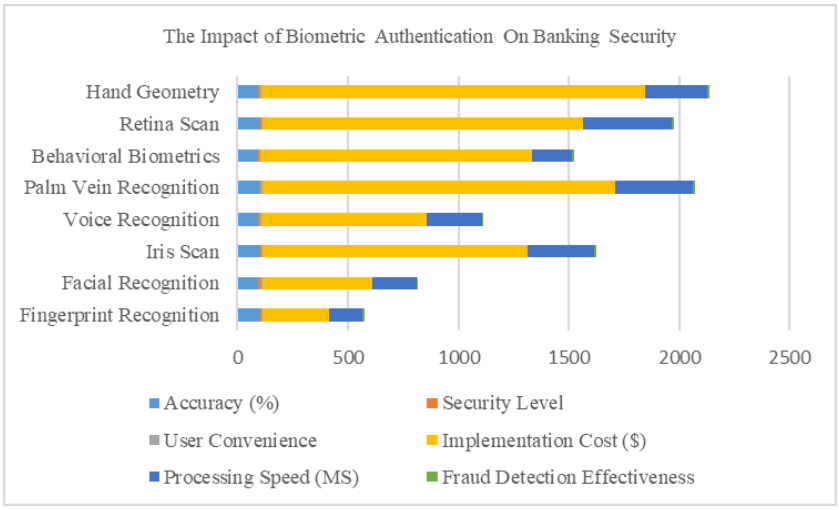


FIGURE 1. The Impact of Biometric Authentication On Banking Security

Figure 1 shows the comparison of biometric authentication techniques using six parameters: accuracy, security, convenience, implementation cost, processing speed, and fraud detection effectiveness. Fingerprint and facial recognition provide a balanced combination of security, accuracy, and convenience. Iris and retina scans achieve superior accuracy and security but require higher investment and offer comparatively lower convenience. Palm vein recognition and behavioral biometrics demonstrate strong security and fraud prevention capabilities, although their costs and processing times may be higher. Voice recognition and hand geometry exhibit moderate performance across the evaluated parameters.

Table 2 presents a comparative evaluation of biometric authentication techniques based on six parameters: accuracy, processing speed, deployment cost, energy consumption, data requirements, and maintenance complexity. Fingerprint recognition provides balanced performance in terms of accuracy, speed, and affordability, making it suitable for banking applications. Iris and retina scans demonstrate higher accuracy and processing speed but involve greater energy consumption and data requirements. Facial recognition offers moderate performance but requires considerable storage and energy resources. Palm vein recognition and hand geometry provide effective fraud detection but involve complex maintenance.

TABLE 2. Normalized Data

Biometric Method	Accuracy (%)	Processing Speed (FPS)	Cost of Deployment ($)	Energy Consumption (W)	Data Requirements (GB)	Maintenance Complexity
Fingerprint Recognition	0.3631	0.3712	0.4169	0.0883	0.1923	0.3546
Facial Recognition	0.3520	0.3299	0.4169	0.1472	0.2564	0.3103
Iris Scan	0.3668	0.4124	0.3243	0.3532	0.3846	0.3989
Voice Recognition	0.3409	0.2887	0.3706	0.2207	0.3205	0.2659
Palm Vein Recognition	0.3594	0.3712	0.2779	0.4709	0.4488	0.3989
Behavioral Biometrics	0.3334	0.2887	0.4169	0.3620	0.2308	0.3103
Retina Scan	0.3668	0.4124	0.2316	0.4267	0.5129	0.4432
Hand Geometry	0.3446	0.3299	0.3243	0.5121	0.3590	0.3103

TABLE 3. Weight

Biometric Method	C1	C2	C3	C4	C5	C6
Fingerprint Recognition	0.25	0.25	0.25	0.25	0.25	0.25
Facial Recognition	0.25	0.25	0.25	0.25	0.25	0.25
Iris Scan	0.25	0.25	0.25	0.25	0.25	0.25
Voice Recognition	0.25	0.25	0.25	0.25	0.25	0.25
Palm Vein Recognition	0.25	0.25	0.25	0.25	0.25	0.25
Behavioral Biometrics	0.25	0.25	0.25	0.25	0.25	0.25
Retina Scan	0.25	0.25	0.25	0.25	0.25	0.25
Hand Geometry	0.25	0.25	0.25	0.25	0.25	0.25

Table 3 presents the weight distribution used for evaluating various biometric authentication methods. Each biometric modality Fingerprint Recognition, Facial Recognition, Iris Scan, Voice Recognition, Palm Vein Recognition, Behavioral Biometrics, Retina Scan, and Hand Geometry has been assigned an equal weight of 0.25 across all six evaluation parameters. This indicates that all criteria are considered equally significant in determining the overall performance of each biometric method in banking security. By applying an equal weighting system, the MOORA method ensures a neutral and unbiased evaluation, allowing each biometric technique to be assessed fairly based on its strengths and weaknesses without prioritizing any specific factor. This approach is particularly useful when the decision-making process requires a balanced consideration of multiple attributes, such as security, accuracy, cost-effectiveness, fraud detection, implementation feasibility, and user convenience.

TABLE 4. Weighted Normalized Decision Matrix

Biometric Method	C1	C2	C3	C4	C5	C6
Fingerprint Recognition	0.0908	0.0928	0.1042	0.0221	0.0481	0.0886
Facial Recognition	0.0880	0.0825	0.1042	0.0368	0.0641	0.0776
Iris Scan	0.0917	0.1031	0.0811	0.0883	0.0962	0.0997
Voice Recognition	0.0852	0.0722	0.0926	0.0552	0.0801	0.0665
Palm Vein Recognition	0.0898	0.0928	0.0695	0.1177	0.1122	0.0997
Behavioral Biometrics	0.0834	0.0722	0.1042	0.0905	0.0577	0.0776
Retina Scan	0.0917	0.1031	0.0579	0.1067	0.1282	0.1108
Hand Geometry	0.0861	0.0825	0.0811	0.1280	0.0898	0.0776

Table 4 presents Each biometric modality is assigned weighted values across six evaluation parameters, providing a comprehensive performance assessment. Iris scan (0.0917, 0.1031, 0.0811, 0.0883, 0.0962, 0.0997) and retina scan (0.0917, 0.1031, 0.0579, 0.1067, 0.1282, 0.1108) show strong performance across security and fraud prevention but may be less convenient or costlier to implement. Fingerprint recognition (0.0908, 0.0928, 0.1042, 0.0221, 0.0481, 0.0886) remains one of the most balanced options, combining security with user convenience and cost-effectiveness. Palm vein recognition (0.0898, 0.0928, 0.0695, 0.1177, 0.1122, 0.0997) and hand geometry (0.0861, 0.0825, 0.0811, 0.1280, 0.0898, 0.0776) rank well in fraud detection and security but might have higher implementation costs. Voice recognition and behavioral biometrics show moderate performance, likely due to their ease of use but potential vulnerabilities. This weighted analysis helps financial institutions make data-driven decisions in selecting the most suitable biometric authentication methods by balancing security effectiveness and practical usability.

TABLE 5. Assessment Value

Biometric Method	Assessment Value
Fingerprint Recognition	0.1290
Facial Recognition	0.0962
Iris Scan	-0.0083
Voice Recognition	0.0482
Palm Vein Recognition	-0.0775
Behavioral Biometrics	0.0340
Retina Scan	-0.0930
Hand Geometry	-0.0457

Table 5 presents the MOORA-based assessment of biometric authentication methods according to accuracy, fraud prevention, implementation cost, user convenience, and processing efficiency. Fingerprint recognition achieves the highest positive value (0.1290), indicating the strongest overall performance among the evaluated alternatives. Facial recognition (0.0962), voice recognition (0.0482), and behavioral biometrics (0.0340) also obtain positive values, demonstrating their potential for banking authentication. In contrast, iris scanning (-0.0083), hand geometry (-0.0457), palm vein recognition (-0.0775), and retina scanning (-0.0930) receive negative values, suggesting limitations in practical implementation, affordability, or convenience. the findings help financial institutions identify suitable biometric technologies by balancing security performance with operational feasibility.

TABLE 6. Rank

Biometric Method	Rank
Fingerprint Recognition	1
Facial Recognition	2
Iris Scan	5
Voice Recognition	3
Palm Vein Recognition	7
Behavioral Biometrics	4
Retina Scan	8
Hand Geometry	6

Table 6 shows the ranking of biometric authentication techniques using the MOORA method, considering accuracy, fraud detection, user convenience, implementation cost, and processing speed. Retina scanning achieves the highest rank (8), demonstrating its strong potential for banking security, while palm vein (7) and hand geometry (6) also show considerable effectiveness. Iris scanning (5) and behavioral biometrics (4) occupy the middle positions. Voice recognition ranks third, followed by facial recognition (2) and fingerprint recognition (1). Although fingerprint technology is widely adopted, its lower ranking may reflect limitations in certain evaluation criteria. MOORA provides a systematic basis for selecting biometric solutions by balancing security, cost, and usability.

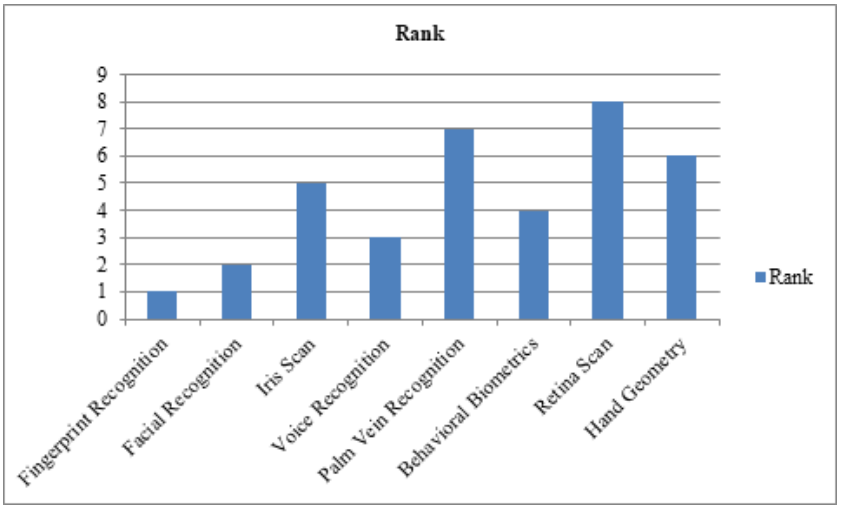


FIGURE 2. Rank

Figure 2 shows the ranking of biometric authentication techniques based on accuracy, security, fraud detection, user convenience, deployment cost, and implementation feasibility. Retina scanning achieves the highest ranking, highlighting its superior security and fraud prevention capabilities. Behavioral biometrics and iris scanning also demonstrate strong performance in authentication reliability. Conversely, fingerprint and facial recognition receive lower rankings according to the evaluated criteria. Hand geometry, palm vein, and voice recognition exhibit moderate performance, indicating acceptable security and usability. Overall, the ranking identifies the strengths and limitations of different biometric technologies, supporting financial institutions in selecting suitable authentication methods for secure, efficient, and cost-effective banking operations.

5. CONCLUSION

Biometric authentication has emerged as a transformative solution in enhancing banking security, significantly reshaping the way financial institutions protect their systems, customers, and sensitive data. As cyber threats and fraudulent activities continue to evolve, the banking sector has recognized the importance of integrating robust, reliable, and user-friendly security measures. Among the various technological advancements, biometric authentication stands out as a highly effective method that not only enhances security but also improves customer convenience. The findings indicate that biometric authentication significantly contributes to strengthening banking security systems while offering a seamless user experience. Iris and retina scans, in particular, have demonstrated exceptional security levels, with accuracy rates reaching up to 99%. These methods are nearly impossible to forge, making them ideal for high-security transactions. The combination of high accuracy rates and rapid processing speeds makes fingerprint recognition a preferred choice for many banking applications. Moreover, biometric authentication helps mitigate identity theft by ensuring that only authorized individuals can access their accounts. Fraud detection effectiveness, as highlighted in the dataset, shows that biometric systems like retina scans and palm vein recognition excel in identifying fraudulent activities. These technologies employ advanced algorithms that detect anomalies in biometric data, flagging suspicious activities and preventing unauthorized transactions. While security is the primary objective of biometric authentication, user convenience plays a crucial role in its widespread adoption. Customers expect seamless, fast, and hassle-free banking experiences, especially in an era where digital banking has become the norm. Fingerprint and facial recognition technologies, in particular, offer exceptional ease of use. These methods can be seamlessly integrated into mobile banking apps and ATMs, allowing customers to authenticate transactions with a simple touch or glance. Behavioral biometrics, which analyze patterns in user behavior such as typing speed or mouse movements, further enhance user experience by providing continuous, unobtrusive authentication without requiring explicit actions from the user. Advanced biometric retina scans, require sophisticated hardware and software infrastructure, making them cost-prohibitive for smaller banks and financial institutions. The dataset highlights the considerable implementation costs associated with these technologies, with retina scans and palm vein recognition ranking among the most expensive

alternatives. On the other hand, fingerprint recognition and behavioral biometrics offer more cost-effective solutions without compromising security. The scalability and affordability of these technologies have contributed to their widespread adoption across the banking sector. Despite the initial costs, the long-term benefits of biometric authentication often outweigh the financial investment. By reducing fraud-related losses, streamlining authentication processes, and enhancing customer trust, biometric systems provide a strong return on investment for banks. Financial institutions must implement robust encryption protocols, secure storage mechanisms, and consent-based data collection practices to safeguard biometric information.

REFERENCES

[1]. Venkatraman, Sitalakshmi, and Indika Delpachitra. "Biometrics in banking security: a case study." Information Management & Computer Security 16, no. 4 (2008): 415-430.

[2]. Palsule, V. (2026). Enhancing Your Communication Skills for Success Used WSM Method. Contemporaneity of English Language and Literature in the Robotized Millennium, 5(2), 44-50. https://doi.org/10.46632/cellrm/5/2/6

[3]. Amin, Hanudin. "Internet banking adoption among young intellectuals." Journal of Internet banking and commerce 12, no. 3 (2007): 1.

[4]. Gubbala, Somasekhar. “SimComment: A Simulation-Guided Hybrid Framework for Efficient Inline Code Comment Smell Detection Using Small and Large Language Models.” In Frontiers in Advanced Computing and Emerging Intelligent Technologies: FACEIT 2026, edited by S. Dehuri, M. K. Patra, S. K. Panda, M. N. Favorskaya, and R. Buyya, vol. 63 of Learning and Analytics in Intelligent Systems. Cham: Springer, 2026. https://doi.org/10.1007/978-3-032-29501-9_11

[5]. Laux, Dawn, Andy Luse, Brian Mennecke, and Anthony M. Townsend. "Adoption of biometric authentication systems: implications for research and practice in the deployment of end-user security systems." Journal of Organizational Computing and Electronic Commerce 21, no. 3 (2011): 221-245.

[6]. Gubbala, Somasekhar. “Hybrid Framework for Efficient Inline Code Comment Smell Detection Using Small and Large Language Models.” In Frontiers in Advanced Computing and Emerging Intelligent Technologies: Proceedings of FACEIT-2026, 109. Springer Nature, 2026.

[7]. Vimala Saravanan, M. Ramachandran, Chitra Periyasamy, Anusuya Mohan, "Performance Evaluation of Humanoid Robot Imitation Skills Using the MOORA Method", Data Analytics and Artificial Intelligence, 5(1), 2025, 164-174.

[8]. Normalini, M. K., and T. Ramayah. "Biometrics technologies implementation in Internet banking reduce security issues?." Procedia-Social and Behavioral Sciences 65 (2012): 364-369.

[9]. Banga, Lavanya, and Samaya Pillai. "Impact of behavioural biometrics on mobile banking system." In Journal of physics: Conference series, vol. 1964, no. 6, p. 062109. IOP Publishing, 2021.

[10]. Manjula Selvam, Vidhya Prasanth, Devipriya Mani, M. Ramachandran, ”Evaluation of SDN-Based Traffic Engineering in Data Center Networks Using the Weighted Product Method” REST Journal on Data Analytics and Artificial Intelligence, 4(4), 2025, 39-49.

[11]. Vangala, Rama Chandra Reddy. “HARD-Graph: A Hierarchical Adaptive Range-Aware Dynamic Graph Framework for Scalable Knowledge and Vector Search Systems.” In Frontiers in Advanced Computing and Emerging Intelligent Technologies: FACEIT 2026, edited by S. Dehuri, M. K. Patra, S. K. Panda, M. N. Favorskaya, and R. Buyya, vol. 63 of Learning and Analytics in Intelligent Systems. Cham: Springer, 2026. https://doi.org/10.1007/978-3-032-29501-9_15.

[12]. Mayayise, Thembekile. "Extending unified theory of acceptance and use of technology with ISO/IEC 27001 security standard to investigate factors influencing Bring Your Own Device adoption in South Africa." South African Journal of Information Management 23, no. 1 (2021): 1-9.

[13]. Khan, Habib Ullah, Muhammad Zain Malik, Shah Nazir, and Faheem Khan. "Utilizing bio metric system for enhancing cyber security in banking sector: A systematic analysis." Ieee Access 11 (2023): 80181-80198.

[14]. Gubbala, Somasekhar, and Rama Chandra Reddy Vangala. Data Lakes to Intelligent Business Analytics: Designing Scalable and Intelligent Data Ecosystems. Vol. 1. Amazon Kindle, 2026, 1–135.

[15]. Xu, Ge, A. Sohail Khan, Ata Jahangir Moshayedi, Xiaohong Zhang, and Yang Shuxin. "The object detection, perspective and obstacles in robotic: a review." EAI Endorsed Transactions on AI and Robotics 1, no. 1 (2022).

[16]. Normalini, M. K., and T. Ramayah. "Trust in internet banking in Malaysia and the moderating influence of perceived effectiveness of biometrics technology on perceived privacy and security." Journal of Management Sciences 4, no. 1 (2017): 3-26.

[17]. Suryadevara, Siva Sai Krishna, and Somesh Nagalla. "Multi-Cloud Program Management For Large Scale Deployment." In 2026 International Conference on Smart Futuristic Technology, pp. 1-8. IEEE, 2026.

[18]. Piotrowska, Anna Iwona, Michał Polasik, and Dariusz Piotrowski. "Prospects for the application of biometrics in the Polish banking sector." Equilibrium. Quarterly Journal of Economics and Economic Policy 12, no. 3 (2017).

[19]. Rathinavelu, G. (2023). A FinTech-Oriented Data Mesh and Lakehouse Architecture for Governed, Real-Time Financial Analytics. The Eastasouth Journal of Information System and Computer Science, 1(01), 288–298. https://doi.org/10.58812/esiscs.v1i01.1308

[20]. Bilal, Muhammad, and Ganesh Sankar. "Trust & Security issues in Mobile banking and its effect on Customers." (2011).

[21]. Nagalla, Somesh, and Soumya Remella. "SLA Driven Program Planning for Cloud Delivery Pipelines." In 2026 International

Conference on Smart Futuristic Technology, pp. 1-11. IEEE, 2026.
[22]. Parusheva, Silvia. "A comparative study on the application of biometric technologies for authentication in online banking." Egyptian Computer Science Journal 39, no. 4 (2015).
[23]. Adesuyi, Falaye Adeyinka, Osho Oluwafemi, ISIAQ OLUDARE Alabi, Adama Ndako Victor, and Amanambu Victor Rick. "Secure authentication for mobile banking using facial recognition." (2013).
[24]. Sarma, Gunajit, and Pranav Kumar Singh. "Internet banking: Risk analysis and applicability of biometric technology for authentication." International Journal of Pure and Applied Sciences and Technology 1, no. 2 (2010): 67-78.
[25]. Dandasi, V. V. "Healthcare Data Warehouse Implementation with Machine Learning Regression Analysis: A Comparative Study of Random Forest, AdaBoost, and XGBoost for Regulatory Compliance Prediction." Journal of Artificial intelligence and Machine Learning 2, no. 2: 1-7.
[26]. Tassabehji, Rana, and Mumtaz A. Kamala. "Evaluating biometrics for online banking: The case for usability." International Journal of Information Management 32, no. 5 (2012): 489-494.
[27]. Gurubasannavar, Suresh Deepak, Varun Venkatesh Dandasi, and Raghavendra Sunku. "Enhancing Smart Home Automation with AI And Topsis-Based Decision Making." International Journal of Information Technology and Management Information Systems (IJITMIS) 16, no. 6 (2025): 1-22.
[28]. Dandasi, V. V. "Evaluating Attack Detection and Prevention in SDN NFV Networks: A Comprehensive Security Solution Analysis." JJournal of Artificial intelligence and Machine Learning 1, no. 3 (2023): 1-7.
[29]. Brauers, Willem Karel, and Edmundas Kazimieras Zavadskas. "The MOORA method and its application to privatization in a transition economy." Control and cybernetics 35, no. 2 (2006): 445-469.
[30]. Karande, Prasad, and Shankar Chakraborty. "Application of multi-objective optimization on the basis of ratio analysis (MOORA) method for materials selection." Materials & Design 37 (2012): 317-324.
[31]. Gaurav Saxena, "Real-Time Predictive Optimization Framework for Multi-Platform Digital Advertising Using Machine Learning and Multi-Criteria Decision Analysis," Journal of Software Quality Engineering and DevOps 1, no. 2 (2026): 1–14.
[32]. Brauers, Willem Karel M. "Multi-objective contractor's ranking by applying the MOORA method." Journal of Business Economics and management 4 (2008): 245-255.
[33]. Gaurav Saxena, "Predicting Code Coverage in DevOps Pipelines Using Machine Learning Regression Models," International Journal of Computer Science and Data Engineering 3, no. 1 (2026): 1–9.
[34]. Gadakh, V. S., Vilas Baburao Shinde, and N. S. Khemnar. "Optimization of welding process parameters using MOORA method." The International Journal of Advanced Manufacturing Technology 69 (2013): 2031-2039.
[35]. Rathinavelu, G. (2025). AI Governance: Automatically Checking AI Systems Against the EU AI Act and NIST Rules. The Eastasouth Journal of Information System and Computer Science, 2(03), 428–438. https://doi.org/10.58812/esiscs.v2i03.1257
[36]. Brauers, Willem K., and Edmundas K. Zavadskas. "Robustness of the multi-objective MOORA method with a test for the facilities sector." Technological and economic development of economy 15, no. 2 (2009): 352-375.
[37]. Gopinathan Rathinavelu. (2025). Real-Time Explainable AI (XAI) and Automated Adverse Action Reporting for Deep Learning Credit Card Decisioning. International Journal of Computational and Experimental Science and Engineering, 11(4). https://doi.org/10.22399/ijcesen.5552