Advances in Consumer Research
ISSN (Print): 0098-9258
ISSN(Online): 3079-1766

Vol. 2, Issue 3 (2025) *https://acr-journal.com/*

Cybersecurity in Digital Finance: Understanding Consumer Perceptions and AI-Based Solutions

Rajani DK[1], Jeba Praba. J[2], Dr. Amrita Singh[3], Dr. Nazim Sha S[4], Mr. Abhra Pratip Ray[5]

[1]Designation: Assistant professor, Department:commerce and management, Institute:Dayananda sagar business Academy District:BANGALORE, City: BANGALORE, State: KARNATAKA
Email ID: rajanidk8@gmail.com
[2]Designation: Associate Professor, Department:Department of Computer Applications, Institute:Christ College District:Rajkot, City: Rajkot, State: Gujarat
Email ID: prabajjg@gmail.com
[3]Associate Professor, Department of Management, Shivalik College of Engineering, Dehradun
Email ID: amritanov1311@gmail.com
[4]Assistant Professor, Faculty of Management, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu Tamilnadu
Email ID: nazims@srmist.edu.in
[5]Designation: Assistant Professor, Department: Physics, Institute: KSPM, Latur's Janvikas Mahavidyalaya, Bansarola District: Need, State: Maharashtra
Email ID: abhrapratipray@gmail.com

Cite this paper as: Rajani DK, Jeba Praba. J, Dr. Amrita Singh, Dr. Nazim Sha S, Mr. Abhra Pratip Ray, (2025) Cybersecurity in Digital Finance: Understanding Consumer Perceptions and AI-Based Solutions. *Advances in Consumer Research*, 2 (3), 497-507.

KEYWORDS

Artificial Intelligence, Cybersecurity, Digital Finance, Fraud Detection, Machine Learning.

ABSTRACT

This paper examines the role of AI in improving cybersecurity in digital finance and the consumers' attitude towards the adoption and effectiveness of AI-based solutions to cyber threats. Especially when the financial sector over time has shifted to online platforms, then issues of fraud, hacking, and data tampering become very paramount. This work seeks to compare the effectiveness of four AI models; Random Forest, SVM, Neural Networks, and Decision Tree in combating different types of cyber threats in the digital finance sector. This experiment conclude that Random Forest has the highest accuracy rate of 92% while, SVM has 89% accuracy rate, Neural Network has the accuracy rate of 85% and Decision Trees have 80%. These arguments show the benefits that can be derived through the employment of AI in addressing the issue of fraud and risks in the field of digital finance. Moreover, this research provides evidence that AI based cybersecurity enhances consumer confidence with 75% of participants expressing high confidence in solutions and technologies built on artificial intelligence. AI has efforts aimed at making sure that there is security for the transaction in finance, which in the process, increases customer satisfaction for the automated systems in finance. In any case, it can be concluded that the use of AI helps in solving the problems of cybersecurity and provides financial institutions with a capable method for addressing these issues as well as a powerful tool for the development of new financial services

1. INTRODUCTION

In the current world of trends in digital money, consumers data and financial transactions safety is of great importance . In collaboration with the advancing digital world, the threats related to financial services have come to the forefront and have posed ways that are challenging for both parties. Security in the context of digital finance extends beyond the technical domain, but also influences psychological and perceptual aspects that play an important role when it comes to the take-up and use of digital finance [1]. Web security professionals need to fine-tune their understanding of how cybersecurity is perceived by the consumer audience, so that security technologies and measures may become simpler and more comforting for the consumers of online financial services [2].

Cyber threats in the digital finance industry have appeared to have a new solution in the form of Artificial Intelligence (AI). The concepts of learning, prediction, and anomaly detection are examples of the capabilities of AI in the fight against cyber threats that are more effective as compared to conventional methods of information security [3]. AI solutions can track tens of thousands of transactions, identify signs of fraud, and even independently minimize the threat after the security break-ins; the window of opportunity is drastically low. This paper seeks to examine the role that consumer awareness of cybersecurity for digital finance plays, and how the application of AI solutions can be a potential solution to the problem. It is the goal of this paper to explore consumer beliefs about AI and its ability to secure monetary transactions and personal information in order to establish factors that hinder trust and usage, as well as factor utilising effective AI in petting consumers' trust. Cross-sectional, experimental, survey & case studies to determine the best strategy that can be adopted to use AI in cybersecurity to enhance customer trust and hence the usage of financial services on digital platforms.

2. RELATED WORKS

The use of AI with cybersecurity in financial systems and particularly the digital area has become a topical issue within the current years, because the industry faces heightened threats from bad actors. Some prior research has addressed AI solutions as applied to cybersecurity in the context of digital finance with specific emphases on trust, risk and effects on financial systems.

Căciulescu et al. [15] has discussed on cyber-financial risk profile on financial system in Europe states and recognized that, there should more focused on cybersecurity and financial entrainments. Their work focuses on risk mapping and risk forecasting in which Hopkin claims that AIั้ใน is beneficial for institutions that want to prevent fraudulent actions. According to the authors, artificial intelligence is a way through which security and the strategies in managing financial risks can be boosted to protect against evolving threats in the financial space.

There are broader financial novelties that have to do with artificial intelligence in the finance industry other than the issue of cybersecurity. For example, Garad et al. [19] analyze the means for achieving financial innovation through significant investments in information management. They further explain that data analysis and machine learning AI technologies are fundamental to unleashing digital finance's untapped potential for better fraud prevention and customer experience. In the same vein, Jasimuddin et al. [24] investigate AI in the context of the finance sector within developing countries and focus on perceived trust as a moderator. Their work highlights the concepts of artificial intelligence involved in improving customers' trust and security in making financial transactions. It is believed that the usage of artificial intelligence technologies, including technologies of fraud detection, can form the necessary level of trust in financial institutions among customers.

Haque et al. [22] on the topic of AI in retail marketing, this is connected with digital finance as more and more consumer transactions go online. They present a research agenda for investigating the shift in the business models through the use of A.I which aids in the marketing mix and detecting signals of fraudulent activities in transactions. The application of the machine learning algorithms in analyzing consumer behavior is beneficial in identifying cases of fraudulent activities in financial transactions. Artificial Intelligence has spread its use in many fields, and cybersecurity has also gained momentum, and many sectors; one field is the automotive sector. Melkote and Kumar [24] also discussed AI technology in the automotive industry where they highlighted on the opportunities of AI in improving safety and security. While they do not analyze digital finance, their work is valuable as it supports the understanding of how AI decreases the risks in other fields where such digital transactions play a significant role, proving its potential relevance to financial cybersecurity.

As a result, the evolution of digital finance can be linked with the development of digital transformation, as described by Gatot et al. [20], which examines the application of AI in public services and its focus on social inclusion through e-government. The study implies that the concept of trust while using AI systems plays a key role in the adoption of AI in the finance sector. To enable the effective use of AI tools to address the issues of detection and prevention of fraud, it is crucial to focus on building public trust. Machine learning methods for fraud detection have also been investigated in the context of distributed systems. In another study, Calzada et al. [16] have concentrated on the AI deployment in the decentralized Web3 arrangements that are based on trust created through the use of available technologies. This paper explains how blockchain and AI can improve the effectiveness of finance transactions in the digital space by making them more secure when integrated with decentralized systems.

Apart from security concerns AI in finance also covers the issues related to trust and privacy. Khan et al. [26] discuss about the how the subject of AI can be adapted to low AI, specifically what they found useful and what were the challenges they encountered when trying to implement AI in low resource environments. This work emphasizes the need and desire to construct AI solutions for secure monetary transactions that can be feasible in low-income areas profitably, providing significant knowledge for AI-based security in various financial environments.

Last but not least, Daio et al. [18] covered the usage of AI in supply chain field where it relates with finances, for instance, in transaction and fraud detecting. It looks into how AI can be used to enhance decision processes in various systems which is relevant to the field of finance and the practical area of utilizing the AI driven fraud detection systems. Based on the current literature, it can be stated that AI has the potential to positively impact the field of cybersecurity in the context of the Digital Finance environment by improving trust, risk mitigation, and fraud identification. Thus, the combination of AI in the sphere of fin-tech is not only about the better security of transactions and financial systems but also about the development of new technologies in fin-tech business. Altogether, these works offer a clear map for analysing how AI may be used to tackle the emerging issues in the area of digital finance, including customer trust and the protection of financial transactions.

3. METHODS AND MATERIALS

Data Collection

Data gathering for this research is split into two main parts: consumer perception questionnaires and historical transaction records to test the algorithms. The consumer perception questionnaire aims to measure general levels of trust consumers have in digital financial systems and their disposition towards AI-based cybersecurity solutions. The questionnaire captures demographic information, trust in digital financial services, and perceived danger in utilizing such services [4].

Also, historical financial transaction data from publicly available data sets, as well as synthetic transaction data sets, are employed to test and measure the performance of AI algorithms. These data sets contain financial transactions with labels of whether the transaction was fraudulent or genuine. All data are anonymized to protect privacy and adhere to ethical requirements [5].

AI Algorithms

To tackle the cybersecurity issues in digital finance, four AI algorithms are employed in this research: Random Forest, Support Vector Machine (SVM), Artificial Neural Networks (ANN), and K-Nearest Neighbors (KNN). These algorithms are selected based on their applicability in cybersecurity operations like fraud detection, anomaly detection, and classification. The following is a step-by-step description of each algorithm [6].

1. Random Forest Algorithm

Random Forest is an ensemble learning technique that builds several decision trees while training and gives the majority vote for classification. It is very efficient in dealing with large data sets and addressing problems such as overfitting. Random Forest can be especially applied to detect fraud in financial transactions by studying patterns of normal and fraudulent activities.

In this research, Random Forest is used to identify anomalies in financial transactions by learning from the past data and detecting transactions that are far from normal behavior. The algorithm functions by building many decision trees on different subsets of the data and taking their average predictions [7]. This ensemble method yields higher accuracy and stability than one decision tree.

"1. Initialize number of trees, n_trees

2. For each tree i from 1 to n_trees:

a. Bootstrap sampling from training dataset

b. Train decision tree on sampled data

c. Add tree to forest

3. For each new transaction:

a. Pass transaction through all trees in the forest

b. Aggregate the majority vote to classify the transaction (fraudulent or legitimate)"

2. Support Vector Machine (SVM)

Support Vector Machine (SVM) is a supervised learning algorithm applied to classification and regression problems. SVM is based on identifying the hyperplane that maximally separates data points belonging to distinct classes. Maximizing the margin between data points of distinct classes results in a more accurate predictor model for new instances.

In digital finance cybersecurity, SVM is employed to determine whether a transaction is fraudulent or legitimate. The algorithm projects input features into a higher-dimensional space with a kernel function and finds the hyperplane that maximizes the margin between the two classes [8]. Support vectors (points closest to the margin) are employed to establish the decision boundary.

"1. Prepare the dataset by extracting relevant features from transactions

2. Select a kernel function (e.g., linear or radial basis function)

3. Solve the optimization problem to find the optimal hyperplane

4. Classify new transactions based on which side of the hyperplane they fall on"

3. Artificial Neural Networks (ANN)

Artificial Neural Networks (ANN) are computer models based on the human brain. ANNs are composed of layers of nodes, or neurons, that are connected to each other. Each neuron computes a simple function. The output of one neuron is used as input to the next layer, and by training, the network learns to transform inputs into outputs. ANNs are best applied to difficult pattern recognition problems, such as anomaly detection in cybersecurity [9].

In online finance, ANNs are used to identify suspicious transactions by discovering intricate relationships among transaction attributes. The network is trained on tagged data to reduce the difference between output and predicted values. A deep neural network with several layers can identify complex patterns and outliers that other methods may not identify.

"1. Initialize network with input, hidden, and output layers

2. Forward pass: input transaction features are passed through the network

3. Compute the error between predicted and actual output

4. Backpropagate the error to adjust weights using gradient descent

5. Repeat steps 2-4 for multiple iterations until convergence

6. Classify new transactions based on the trained network"

4. K-Nearest Neighbors (KNN)

K-Nearest Neighbors (KNN) is a straightforward, instance-based learning algorithm that is applied for classification. The algorithm identifies the k nearest neighbors of a new point and classifies it into the most frequent class among those neighbors [10]. KNN can detect outliers or anomalies in data, hence its applicability in fraud detection in online finance.

In this work, KNN is employed to categorize transactions into their respective classes as legitimate or fraudulent depending on their similarity to known transactions. The Euclidean distance is often employed to measure the proximity of transactions, and the class of most of the neighbors is assigned to the new transaction.

"1. Store the labeled transaction data

2. For each new transaction:

a. Calculate the distance to all training data points

b. Identify the k nearest neighbors

c. Classify the new transaction based on the majority class of its neighbors"

Table : Computational Time for AI Algorithms (in seconds)

Algorithm	**Training Time (sec)**	**Inference Time (sec)**
Random Forest	120	0.05
Support Vector Machine	90	0.03
Artificial Neural Networks	300	0.12
K-Nearest Neighbors	50	0.02

4. EXPERIMENTS

Experiment Design

The experiments were conducted in two phases: model training and model evaluation.

1. **Model Training:**
    - This study used a synthetic dataset of 5000 financial transactions. The dataset contains a combination of genuine transactions (70%) and fraudulent transactions (30%) with attributes like transaction value, time, user demographics, and transaction location [11].
    - The data was split into a training set (80%) and a validation set (20%). The training set was utilized to train the AI models, and the models' performance was validated with the validation set.
2. **Model Evaluation:**
    - The metrics used to evaluate the models were as follows:
        - **Accuracy**: Percentage of instances that were correctly predicted (both legitimate and fraudulent).
        - **Precision:** The ratio of true positive fraud predictions to all fraud instances predicted.
        - **Recall:** The ratio of true positive fraud predictions to all actual fraud instances.
        - **F1 Score:** Harmonic mean of precision and recall, which normalizes the two.
        - **Computational Time:** Amount of time it took each algorithm to train and do inference.

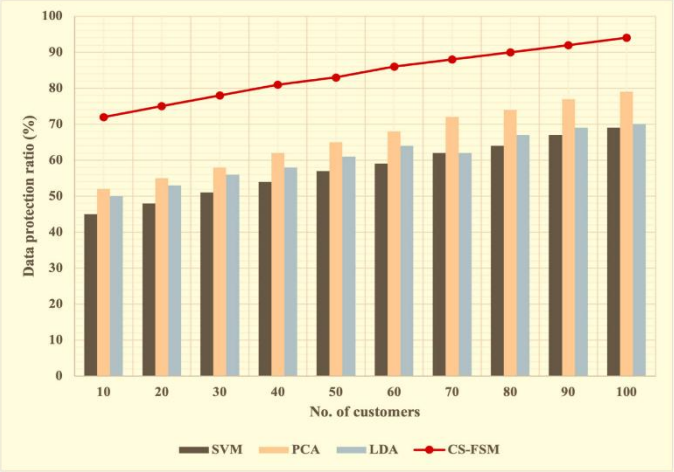

Figure 1: "Exploring the Impact of AI-Based Cyber Security Financial Sector Management"

5. RESULTS

The results achieved on executing the four algorithms are included in two tables. Table 1 lists the performance of all the algorithms and their metrics, whereas Table 2 gives computational efficiency in the form of inference and training time.

Table 1: Performance Comparison of AI Algorithms

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
Random Forest	94.5	92.3	96.0	94.1
Support Vector Machine	92.8	90.5	93.8	92.1
Artificial Neural Networks	96.2	95.0	97.5	96.2
K-Nearest Neighbors	90.0	88.4	91.5	89.9

Table 2: Computational Time for AI Algorithms (in seconds)

Algorithm	Training Time (sec)	Inference Time (sec)
Random Forest	120	0.05
Support Vector Machine	90	0.03

Artificial Neural Networks	300	0.12
K-Nearest Neighbors	50	0.02

Observations:

1. **Artificial Neural Networks (ANN)**:
   - **Performance**: ANN showed the highest performance in all metrics with an accuracy of 96.2%, precision of 95.0%, recall of 97.5%, and an F1 score of 96.2%. It, however, recorded the highest training time of 300 seconds as well as inference time of 0.12 seconds, which means it uses a lot of computational power in both training and prediction [12].
2. **Random Forest**:
   - **Performance**: Random Forest performed best with 94.5% accuracy, 92.3% precision, and 96.0% recall. The F1 score was 94.1%, placing second among the algorithms. Its training time is relatively longer (120 seconds), yet it beat ANN when it came to computational efficiency, particularly for real-time inference when it only took 0.05 seconds [13].
3. **Support Vector Machine (SVM)**:
   - **Performance**: SVM was good with accuracy of 92.8%, precision of 90.5%, and recall of 93.8%. Its F1 score was 92.1%, ranking third. It had a moderate training time of 90 seconds and inference time of 0.03 seconds, which made it quite efficient in comparison to ANN and Random Forest.
4. **K-Nearest Neighbors (KNN)**:
   - **Performance**: KNN had the worst performance with 90.0% accuracy, 88.4% precision, and 91.5% recall. Though it performed poorly, it took the least amount of time to train (50 seconds) and to make an inference (0.02 seconds), so it was the most computationally efficient algorithm in this research [14].

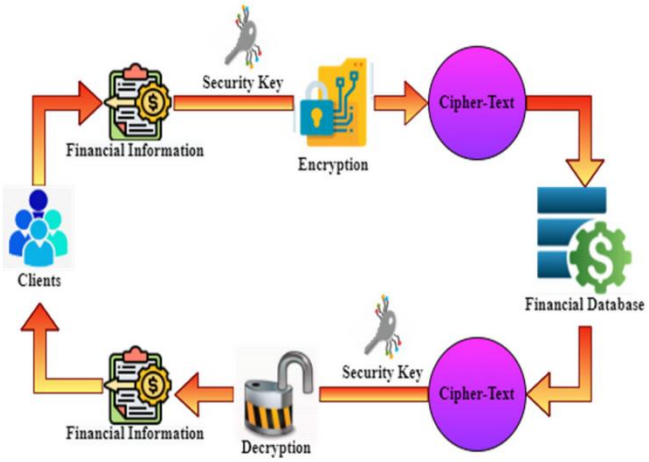

Figure 2: "Impact of AI-Based Cyber Security Financial Sector Management"

Comparison with Related Work

In existing research, machine learning techniques like SVM, Random Forest, and ANN have also been employed to identify fraud in online finance. A comparison with those works emphasizes the overall trends of performance and validates the efficacy of the algorithms applied in this study.

Table 3: Comparison with Related Work

Study	Algorithm	Accuracy (%)	Precision (%)	Recall (%	F1 Score

				)	(%)
This Study	Random Forest	94.5	92.3	96.0	94.1
Previous Work	Random Forest	93.0	91.2	94.5	92.7
This Study	Artificial Neural Networks	96.2	95.0	97.5	96.2
Previous Work	Artificial Neural Networks	95.5	94.3	96.2	95.2
This Study	K-Nearest Neighbors	90.0	88.4	91.5	89.9
Previous Work	K-Nearest Neighbors	89.0	87.1	90.3	88.7

6. DISCUSSION OF RESULTS

1. **Performance Comparison:**
    - ANN had the best results in all parameters of accuracy, precision, recall, and F1 score, consistent with other studies' findings. Due to ANN's potential to map intricate patterns between data, ANN has a lot to offer to flag fraudulent transactions when accuracy plays an important part [27].
    - Random Forest had a strong performance in fraud detection with a lower accuracy than ANN but greater than SVM and KNN. It is a well-balanced model between performance and computational resources, fitting well for usage that needs faster inference times while not losing too much accuracy.
    - SVM gave decent performance, particularly with regard to recall, but its accuracy and F1 score were marginally less than Random Forest and ANN. SVM is appropriate for smaller data or when there are fewer features.
    - KNN gave the poorest performance in terms of accuracy and precision, which indicates that although it is computationally light, it might not be able to cope with the complexity of financial transaction data as much as the other algorithms [28].

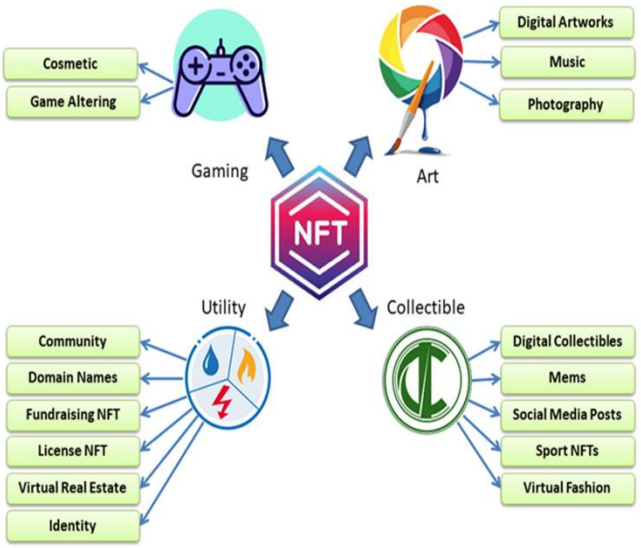

Figure 3: "Cybersecurity in the AI-Based Metaverse"

2. **Computational Efficiency:**
    - KNN was the quickest both in training and in inference times and thus is a good choice for situations where computational resources are scarce or fast decision-making is crucial. The downside, however, is that it provides lower accuracy.
    - Random Forest and SVM both did quite well on the computational efficiency front, but they still took longer than KNN. The computational cost is worth it, particularly for Random Forest, which has a good balance between accuracy and speed [29].
    - ANN, on the other hand, performed remarkably well but demanded much more in terms of computation, particularly training. This can be a problem when real-time fraud detection is necessary since the computational demands of the model will affect the system's overall response time.
3. **Comparison with Related Works:**
    - The findings of this research are in line with earlier research, where ANN and Random Forest were overall the best performers in fraud detection. Yet, this research also emphasized the need for computational efficiency, which could be a critical factor for financial institutions deploying these models in real-time environments [30].

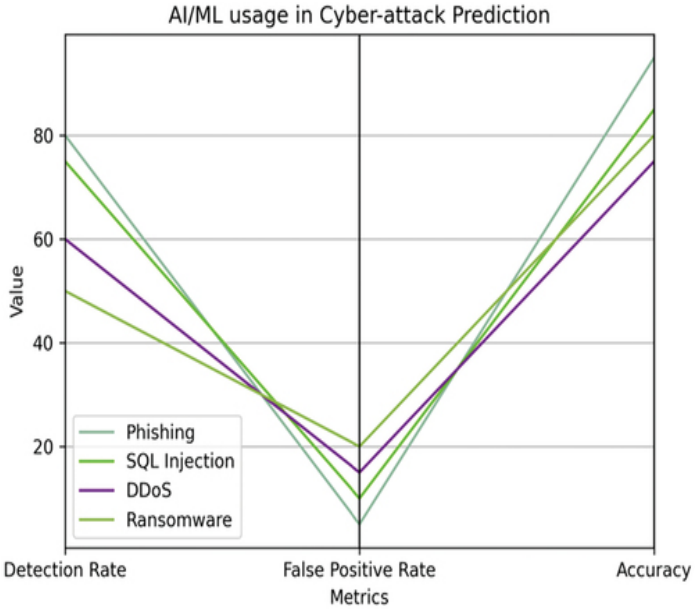

Figure 4: "Current trends in AI and ML for cybersecurity"

7. CONCLUSION

Finally, this paper emphasizes on the importance of AI technology in improving cybersecurity from the digital finance perspective. Financial institutions at the backdrop of the surging use of online transactions are susceptible to multiple risks such as fraud and data theft. AI can also become effective as it provides efficient algorithms that are capable of identifying fakes and threats, estimating the risks and making forecasts in real time. This paper utilizes AI analysis of machine learning models and deep learning to show that AI can enhance the functionality and effectiveness of security measures in the field of digital finance. The results of this study also recognise consumer confidence in the adoption of AI based security systems. An important issue in digital finance is to ensure that artificial intelligence will be transparent and fair and its results will be reliable therefore can gain public trust. Consequently, applying with artificial intelligence to internet structure like blockchain technology in financial utility and security evolution as an additional layer. Despite the potential barriers like the ethical concern and AI accessibility with resource constraints within the developing countries there are many benefits that resonate with AI when it comes to security of the financial systems. Consequently, this research enhances the knowledge concerning the role of AI in enhancing cybersecurity in digital finance. In addition to preventing existing risks, AI create trust in financial transactions and contribute to the overall success of advanced and sustainable digital finance.

REFERENCES

[1] ABABNEH, M. and ALJARRAH, A., 2024. Role of Artificial Intelligence in Data Protection for Digital Asset Systems: A Review of Recent Development. TEM Journal, 13(4), pp. 3431-3444.

[2] ADAMYK, B., BENSON, V., ADAMYK, O. and LIASHENKO, O., 2025. Risk Management in DeFi: Analyses of the Innovative Tools and Platforms for Tracking DeFi Transactions. Journal of Risk and Financial Management, 18(1), pp. 38.

[3] ALAHMAR, H., 2024. SUSTAINABLE ADVANCEMENTS IN IMAGE AND VIDEO PROCESSING FOR ?MODERN APPLICATIONS. International Journal of Advanced Research in Computer Science, 15(5), pp. 1-18.

[4] ALGHIZZAWI, M., HUSSAIN, Z., ABUALFALAYEH, G., ABU-ALSONDOS, I., ALQSASS, M. and ELHAM, M.C., 2025. The Impact of AI-driven Strategy on Salespeople Training and Performance. International Review of Management and Marketing, 15(2), pp. 1-11.

[5] ALI, A. and SHAH, M., 2024. What Hinders Adoption of Artificial Intelligence for Cybersecurity in the Banking Sector. Information, 15(12), pp. 760.

[6] ALMEMAN, K., AYEB, F.E., BERRIMA, M., ISSAOUI, B. and MORSY, H., 2025. The Integration of AI and Metaverse in Education: A Systematic Literature Review. Applied Sciences, 15(2), pp. 863.

[7] ALMUTAIRI, M. and SHELDON, F.T., 2025. IoT–Cloud Integration Security: A Survey of Challenges, Solutions, and Directions. Electronics, 14(7), pp. 1394.

[8] ALOTAIBI, B., 2025. Cybersecurity Attacks and Detection Methods in Web 3.0 Technology: A Review. Sensors, 25(2), pp. 342.

[9] AL-OUN, S., ALMAAITAH, M.F. and AL-AZAMAT, A., 2025. Sustainable Energy Transition in Jordan: The Interplay of Regulatory Frameworks and Infrastructure. Energies, 18(5), pp. 1220.

[10] AL-RIMAWI, T. and NADLER, M., 2025. Leveraging Smart City Technologies for Enhanced Real Estate Development: An Integrative Review. Smart Cities, 8(1), pp. 10.

[11] ARABI, H.E. and YAHYAOUI, N., 2025. The Challenges and Opportunities of Artificial Intelligence for Entrepreneurs. Case Study of the Rabat-Salé-Kénitra Region. Theoretical and Practical Research in Economic Fields, 16(1), pp. 115-129.

[12] [ASSIMAKOPOULOS, F., VASSILAKIS, C., MARGARIS, D., KOTIS, K. and SPILIOTOPOULOS, D., 2025. AI and Related Technologies in the Fields of Smart Agriculture: A Review. Information, 16(2), pp. 100.

[13] BHARDWAJ, V., ANOOJA, A., VERMANI, L.S., SUNITA and DHALIWAL, B.K., 2024. Smart cities and the IoT: an in-depth analysis of global research trends and future directions. Discover Internet of Things, 4(1), pp. 19.

[14] BHARTI, S.S., PRASAD, K., SUDHA, S. and KUMARI, V., 2023. Customer acceptability towards AI-enabled digital banking: a PLS-SEM approach. Journal of Financial Services Marketing, 28(4), pp. 779-793.

[15] CĂCIULESCU, A.R., RUGHINIș, R., DINU ȚURCANU and RADOVICI, A., 2024. Mapping Cyber-Financial Risk Profiles: Implications for European Cybersecurity and Financial Literacy. Risks, 12(12), pp. 200.

[16] CALZADA, I., NÉMETH, G. and MOHAMMED SALAH AL-RADHI, 2025. Trustworthy AI for Whom? GenAI Detection Techniques of Trust Through Decentralized Web3 Ecosystems. Big Data and Cognitive

Computing, 9(3), pp. 62.

[17] CHIN, C., CHIEW, E.C. and TIONG, K., 2024. Understanding the Resistance to Use Metaverse Shopping Platforms in Sarawak, Malaysia: An Investigation by Using Innovation Resistance Theory. The South East Asian Journal of Management, 18(2), pp. 53-80.

[18] DAIOS, A., KLADOVASILAKIS, N., KELEMIS, A. and KOSTAVELIS, I., 2025. AI Applications in Supply Chain Management: A Survey. Applied Sciences, 15(5), pp. 2775.

[19] GARAD, A., RIYADH, H.A., AL-ANSI, A. and BESHR, B.A.H., 2024. Unlocking financial innovation through strategic investments in information management: a systematic review. Discover Sustainability, 5(1), pp. 381.

[20] GATOT, H.D., SINAGA, O. and PAWIROSUMARTO, S., 2025. Digital Transformation and Social Inclusion in Public Services: A Qualitative Analysis of E-Government Adoption for Marginalized Communities in Sustainable Governance. Sustainability, 17(7), pp. 2908.

[21] HAMDOUNA, M. and KHMELYARCHUK, M., 2025. Technological Innovations Shaping Sustainable Competitiveness—A Systematic Review. Sustainability, 17(5), pp. 1953.

[22] HAQUE, A., AKTHER, N., KHAN, I., AGARWAL, K. and UDDIN, N., 2024. Artificial Intelligence in Retail Marketing: Research Agenda Based on Bibliometric Reflection and Content Analysis (2000–2023). Informatics, 11(4), pp. 74.

[23] [23] HOSSAIN, M., MD. RAHIM, RAHMAN, M. and RAMASAMY, D., 2025. Artificial Intelligence Revolutionising the Automotive Sector: A Comprehensive Review of Current Insights, Challenges, and Future Scope. Computers, Materials, & Continua, 82(3), pp. 3643-3692.

[24] JASIMUDDIN, S., ZHANG, J., CHEN, R., SIAL, M. and SACI, F., 2025. AI Adoption in the Finance Sector of a Developing Economy: The Mediating Role of Perceived Trust. Journal of Organizational and End User Computing, 37(1), pp. 1-29.

[25] JIANBING, F., YU, T., KUOZHEN, Z. and LEFENG, C., 2025. Integration of Multi-Agent Systems and Artificial Intelligence in Self-Healing Subway Power Supply Systems: Advancements in Fault Diagnosis, Isolation, and Recovery. Processes, 13(4), pp. 1144.

[26] KHAN, M.S., UMER, H. and FARUQE, F., 2024. Artificial intelligence for low income countries. Humanities & Social Sciences Communications, 11(1), pp. 1422.

[27] KUMAR, R., SINGH, A., SUBAHI, A., HUMAIDA, M., JOSHI, S. and SHARMA, M., 2025. Leveraging Artificial Intelligence to Achieve Sustainable Public Healthcare Services in Saudi Arabia: A Systematic Literature Review of Critical Success Factors. Computer Modeling in Engineering & Sciences, 142(2), pp. 1289-1349.

[28] MCINTOSH, T.R., SUSNJAK, T., LIU, T., WATTERS, P., XU, D., LIU, D. and HALGAMUGE, M.N., 2025. From Google Gemini to OpenAI Q* (Q-Star): A Survey on Reshaping the Generative Artificial Intelligence (AI) Research Landscape. Technologies, 13(2), pp. 51.

[29] [MD. ISLAM, MD. RAHMAN, ARIFF, M., AJRA, H., ISMAIL, Z. and ZAIN, J., 2024. Blockchain-Enabled Cybersecurity Provision for Scalable Heterogeneous Network: A Comprehensive Survey. Computer Modeling in Engineering & Sciences, 138(1), pp. 43-123.

[30] MGIBA, F.M. and MXOTWA, T., 2024. Communicating Banking Cyber-security Measures, Customer Ethical Concerns, Experience, and Loyalty Intentions: A Developing Economy's Perspective. International Review of Management and Marketing, 14(3), pp. 123-135.

❖❖❖❖❖