SECURING FINANCIAL TRANSACTIONS: EXPLORING THE ROLE OF AI-DRIVEN TECHNOLOGICAL INFLUENCES IN ENHANCING SECURITY AND TRUST

Nazia Sultana, Osmania University, Hyderabad, Telangana
Niraj Kishore Chimote, ICFAI Business School, IFHE Hyderabad
Hardeep Singh, Amritsar Group of Colleges, Amritsar (Punjab)
Usman Ghani, Jain Online Deemed to be University, Bengaluru
Mohammad Anwar, Trinity Institute of Professional Studies, New Delhi
Shahid Ameen, Institute of Technology and Management Gwalior, Madhya Pradesh

ABSTRACT

The study's main goal was to assess how AI-driven technologies may improve security and trust by mitigating the negative effects of financial transaction security. Data was gathered using structured questionnaires categorized by gender and income that were mailed to respondents. Purposive sampling was used to collect data from 391 respondents. In the study, regression testing was employed as a quantitative technique to extract statistical insights from the subjects. The results of the step-wise regression analysis showed that the factors under investigation are significant predictors of the Financial Transaction Security (FTS). The beta value of 0.978, according to the coefficient summary, indicates their effect on Financial Transaction Security (FTS) and their extra contribution to Enhanced Trust (ENT).

In summary, the financial services sector presents a revolutionary chance to enhance security protocols by incorporating artificial intelligence (AI). Enhancing trust and security in financial transactions is one of the main advantages of incorporating AI. Security measures, dangers, and the financial ecosystem are all improved by fusing blockchain's transparent and secure platform with AI-powered fraud detection, identity verification, and smart contract automation. This study not only established the relationship between privacy issues and AI in the finance sector, but it also offered recommendations for enhancing data security and protection. Additionally, the document provides fintech organizations with best practices and strategies to ensure data security and privacy. Regulators, financial institutions, and other interested parties who wish to ensure that artificial intelligence is used in the digital finance industry in a way that is morally and responsibly should take note of these findings.

Keywords: Fraud Detection and Prevention (FDP); Real-Time Transaction Monitoring (RTM); Automating Risk Management (ARM); Chatbots and Virtual Assistants (CVA);Financial Transaction Security (FTS); Enhanced Trust (ENT); Artificial Intelligence.

INTRODUCTION

Ensuring the security and credibility of transactions is essential in the rapidly evolving financial technology industry (FinTech) (Olweny, 2024; Smith & Liu, 2024). Financial

Citation Information: Sultana, N., Chimote, N.K., Singh, H., Ghani, U., Anwar, M., & Ameen, S. (2025). Securing financial transactions: exploring the role of ai-driven technological influences in enhancing security and trustl. *Academy of Marketing Studies Journal, 29*(4), 1-20.

institutions are always searching for novel strategies to get better security and lower the risks brought on with the increase in digital transactions and the sophistication of cyberattacks. Using Technology related to artificial intelligence (AI) is one way to address this issue, since it provides a revolutionary means of enhancing security in the financial services industry (Abdel-Rahman, 2023). Kafi & Akter (2023) define artificial intelligence (AI) as the computer equivalent of human intellect, which enables computers to perform tasks like learning, thinking, and problem-solving that otherwise need human intellect. The set of techniques known as Computers with artificial intelligence (AI) can assess data, interpret it, and come to intelligent conclusions on their own. Computer vision, natural language processing, and machine learning are some of these techniques (Nzuva, 2019).

Within the financial services sector, security is crucial since maintaining transaction integrity and safeguarding stakeholders' and customers' interests depend on confidence and secrecy (Chahal, 2023). Financial institutions are susceptible to a wide range of security risks, including as identity theft, cyberattacks, fraud, and data breaches, all of which can cause financial losses, harm to their reputations, and legal ramifications (Bouchama & Kamal, 2021). Thus, putting strong security measures in place is vital to protecting private financial data, maintaining confidence, and guaranteeing the constancy and resilience of the monetary system (Girija, et. al., 2023).

AI integration offers a synergistic way to improve financial services security. Financial institutions can create creative answers to an assortment of safety issues, encompassing Regulatory conformity, risk administration, identity verification, and fraud detection, by utilizing the capabilities of artificial intelligence (Shinde et al., 2023). AI algorithms provide computers the ability to instantly evaluate enormous volumes of data, spotting trends, abnormalities, and questionable activity It might indicate fraud. Meanwhile, AI (artificial intelligence) technological ensures the accuracy and consistency of financial data via offering An open and safe platform for transaction recording and verification (Tyagi et al., 2020). AI offers a powerful combination that transforms the provision and use of financial services by improving security, transparency, and confidence in financial transactions.

Existing literature extensively covers the adoption and acceptance of financial transaction services. However, a notable gap in research emerges regarding the connection between customer ecstasy and the enduring usage patterns of financial transaction services over an long time frame. There is a wealth of study on initial adoption and acceptance, but little is known about the relationship between users' great joy or satisfaction and their sustained and regular usage of financial transaction services across time (Duy Phuong et al., 2020). This paucity of examination into the prolonged usage characteristics in connection to consumers' emotional states provide a substantial topic for additional analysis and academic research in the area of financial transaction services as well as consumer conduct. Filling in these research gaps could provide a more thorough understanding of the relationships found between various components and customer satisfaction in financial transaction services. By concentrating on important components within these insights, efforts to improve customer happiness could be further refined financial transaction services (Kavitha and Rajini, 2024).

While the financial transaction industry isnow using AI more and more, still there are only few comprehensive studies available on the moral and legal implications various applications of AI. There is a need for future studies that may look into financial security concerns and into ethical problems concerning algorithmic bias, data privacy, transparency, and responsibility in artificial intelligence (Nasr et. al., 2020). Although AI techniques have several

Citation Information: Sultana, N., Chimote, N.K., Singh, H., Ghani, U., Anwar, M., & Ameen, S. (2025). Securing financial transactions: exploring the role of ai-driven technological influences in enhancing security and trustl. *Academy of Marketing Studies Journal, 29*(4), 1-20.

potential to get better financial modelling and evaluation, still further Research is required to find the optimal strategies to combine AI with traditional financial transaction models. The present research will examine hybrid strategies that combine algorithms for artificial intelligence (AI) with conventional models of econometry to enhance risk control and fraud detection in the monetary transaction services sector (Lai & Tong, 2022).

LITERATURE REVIEW

The financial technology industry has advanced significantly recently thanks to digitisation and big data analytic combination, cloud computing, and synthetic intelligence (AI) (Liyanaarachchi et al., 2020). Financial entities such as banks can offer their customers services that are more flexible and convenient thanks according to Malaquias and Hwang (2019), financial technology. Fintech leverages mobile gadgets and additional technology platforms to enable customers to take part in a variety of financial activities, quickly access their bank accounts and get alerts about transactions (Yu and Song, 2021).

One of the key elements propelling AI's growth within the fintech industry is its capacity to handle massive quantities of information and extract meaningful information for making decisions (Daníelsson et al., 2022). By integrating AI with big-data analytics, Fintech businesses can acquire an advantage over competitors in the market by providing customized monetary services, increasing efficiency of operations, and reducing costs (Yang et al., 2022). Nevertheless, the application of AI and large data set in the finance sector brings up privacy and ethical issues.

The financial industry's use of big data, AI, and privacy has sparked debates over how crucial it is to take ethical issues into account. Bias, prejudice, privacy, openness, fairness, ownership, and control are some of these factors (Saltz and Dewar, 2019). As insufficient or biased data inputs can lead to discriminatory or unfair findings that have a significant impact on people, it is imperative to ensure fairness in decision-making processes (Daníelsson et al., 2022). Additionally, openness in the gathering, use, and analysis of data is crucial for preserving client reputation, claim Vannucci and Pantano (2020). Additionally, protecting personal information and abiding with Regulations and legislation pertaining to data privacy are moral issues for fintech businesses (La Torre et al., 2019; Mangla and Parkar 2021).

The intricate connection between fintech and consumer another is trust. Crucial issue that must be taken into account. Trust is a major Another element in the uptake of fintech services is trust, especially in relation to data security and privacy (Liyanaarachchi et al., 2020). Due to worries about data breaches and online banking vulnerabilities, customers are now reluctant to conduct financial transactions through fintech platforms (Abed and Anupam, 2022). To foster customer confidence and encourage broader fintech service adoption, Data Concerns about privacy and security must be addressed. (Laksamana et al., 2022). In the age of fintech, methods for encouraging trust within Fintech businesses have been suggested as a means of addressing the trust deficit. One such strategy is the adoption of AI, which highlights the moral and responsible use of information and technology breakthroughs (Jelovac et al., 2021). Fintech enterprises have the ability to create and preserve digital trust through highlighting the good impacts of technology on society and making sure that data processing is done ethically. Organizations can enhance their reputation, customer happiness, digital trust, and financial success by implementing AI (Herden et al., 2021).

Citation Information: Sultana, N., Chimote, N.K., Singh, H., Ghani, U., Anwar, M., & Ameen, S. (2025). Securing financial transactions: exploring the role of ai-driven technological influences in enhancing security and trustl. *Academy of Marketing Studies Journal, 29*(4), 1-20.

Within the fintech sector, adopting technological solutions is crucial for both regulatory compliance and successfully protecting consumer data. To ensure that private data is safe and unreadable during transmission and storage, for instance, encryption techniques are crucial (Laksamana et al., 2022). By using robust encryption, financial technology firms can lower their danger of data breaches and stop un-authorised entry into customer information. Furthermore, using multifactor authentication methods like biometrics or token-based systems has two advantages: it lowers the chance of prevents unwanted entry and provides an additional degree of protection to client accounts (Yang et al., 2022). Both opportunities and difficulties arise from the fintech industry's use of AI. Although new financial services and improved customer experiences are made possible by these technologies, it is crucial to discuss moral issues such bias, transparency, privacy, and trust (Nasr et al., 2020). Building trust, protecting consumer privacy, and promoting the sustainable expansion of the financial industry are all possible for financial organizations through implementing secure technical solutions, adhering to legal frameworks, and emphasizing the moral and responsible application of data. In order to create a fintech ecosystem that is moral and privacy-conscious, stakeholders must work together (Alam et al., 2020).

This study examines data privacy flaws in the financial technology sector through content analysis. The gathered research was divided into four major themes using an analysis method. The analysis's conclusions show how important data security and privacy are to fostering consumer confidence and enhancing a company's reputation.

Fraud Detection and Prevention (FDP)

Institutions of finance continue to have serious concerns about fraud because cybercriminals are always developing new strategies to take advantage of holes in systems and procedures. According to Liao et al. (2020), detection of fraud and prevention systems that are driven by synthetic intelligence (AI) employ machine learning algorithms to scan substantial quantities of transactional data and identify fraudulent activity instantly. These technologies are able To find trends that indicate fraudulent activity, like odd amounts of transactions, strange spending patterns, or shady attempts to log in. AI programs are able to identify possible fraud alarms by keeping a close eye on transactions and user conduct. This allows financial organisations to take prompt action to reduce risks and safeguard their clients (Wang and He, 2020). Additionally, with emerging fraud trends develop risks emerge, AI-driven Systems for detecting fraud may adjust and gain knowledge from them gradually increasing their accuracy and effectiveness. Financial institutions can reduce financial losses and remain ahead of changing fraud strategies with this dynamic approach (Reim et al., 2020).

Increasing Efforts to prevent fraud and maintain cyber security are growing vital for any bank or financial organisation because of the large volume of electronic everyday transactions using internet accounts, often utilising apps and mobile devices (Irshad. & Neha 2013; Lopes and Pereira, 2019b). The increasing security of internet banking is mostly due to AI. Thanks to AI's ability to offer this degree of protection for individuals at the base of the financial inclusion pyramid can now use online banking participate in the formal financial sector (Reim et al., 2020). Moreover, AI technology is being used by financial firms in various countries to detect fraud, enhance user experience and consumer protection, and limit risk (Ray et al., 2019). To get better oversight and stop their trading at high frequencies from being manipulated systems, several National stock markets throughout the world are considering using machine learning techniques to spot trends in the market (Hassani et al., 2020). Actually, there is a growing trend

Citation Information: Sultana, N., Chimote, N.K., Singh, H., Ghani, U., Anwar, M., & Ameen, S. (2025). Securing financial transactions: exploring the role of ai-driven technological influences in enhancing security and trustl. *Academy of Marketing Studies Journal, 29*(4), 1-20.

toward the use of AI-enabled cybersecurity technology to prevent and detect possible security breaches. Additionally, Advisors that are robots—which offer services for automated financial planning including advice on investments, insurance, taxes, and health—among many other essential services—are another way that artificial intelligence is influencing wealth management (Alameda, 2020). Artificial intelligence (AI) is employed by Indian banks in their mobile banking applications and On Chat, a chat platform that facilitates communication, confirmation, and payment for services through natural language processing (Ray et al., 2019).

H1a: *FDPhassignificantpositive impact on FTS*

H1b: *AI moderate the relationship between FDP and FTS*

Real-Time Transaction Monitoring (RTM)

By facilitating a safe and easy transaction process, real-time monitoring solutions not only reduce fraud but also increase client happiness. In order to effectively combat fraud in the current digital age, firms must implement proactive fraud prevention methods (Hassan et al., 2023). Organisations can mitigate the risk of fraudulent activities by utilising predictive analytics to identify possible hotspots and putting preventive measures in place. By giving immediate signals for questionable activity and facilitating quick responses to reduce fraud, real-time monitoring systems significantly improve efforts to prevent fraud. Combining these preventive tactics enables businesses to keep One step forward of fraudsters and protect their resources and clients from dishonest behavior (Rakha, 2023).

Real-time pattern identification and anomaly detection are two areas where AI algorithms shine in the context of transaction security. They examine transaction data closely in order to identify trends that could indicate fraud. For example, rapid purchases from different locations may indicate an effort to use a credit card that has been stolen (Świątkowska, 2020). Similar to this, AI algorithms monitor spending patterns and are able to quickly spot anomalous purchases or abrupt increases in spending as possible warning signs (Thakur, 2024). In order to identify suspicious activity, they also examine the temporal elements of transactions, evaluating variables like time, frequency, and location.

H2a: *RTMhas significantnegative impact on FTS*

H2b: *AI moderate the relationship between RTM and FTS*

Chatbots and Virtual Assistants (CVA)

The chatbot is currently the most evident application of AI. Reim et al. (2020) define a chatbot as an innovative administrative tool driven through algorithms that interacts with a customer in a distinctive (human-like) manner through voice or content. Certain chatbots are assigned virtual operator personalities, which may include names, symbols, and characters. More and more consumer concerns are being handled by chatbots and virtual assistants, who offer prompt and precise answers. Consequently, clients are more satisfied and care Agents are working less (Lopes and Pereira, 2019b). It involves evaluating the complexity and efficacy regarding artificial intelligence (AI) algorithms, analytics of data skills, and technical infrastructure that businesses use to provide creative financial solutions (Ray et al., 2019). The application regarding artificial intelligence (AI) by banks to provide help desks and customer

Citation Information: Sultana, N., Chimote, N.K., Singh, H., Ghani, U., Anwar, M., & Ameen, S. (2025). Securing financial transactions: exploring the role of ai-driven technological influences in enhancing security and trustl. *Academy of Marketing Studies Journal, 29*(4), 1-20.

service, which has a bigger influence on efficiency and cost savings. Banks are now offering electronic virtual assistants, and financial institutions can provide customised banking with AI helpers and chat bots that leverage processing of natural language to provide quick, self-help client support and artificial intelligence (AI) to generate individualised financial guidance (Alameda 2020). Banks are going over and above by introducing chatbots that use AI to manage relationships.

H3a: *CVAhas significantimpact on FTS*

H3b: *AI moderate the relationship between CVA and FTS*

Automating Risk Management (ARM)

Many vulnerable populations, like women, young people, and small enterprises, like small-scale farmers, were not included in the official conventional banking industry's financial market because in large part to risk concerns (Frank, 2019). They were considered high risk since many of these vulnerable populations were difficult to identify and evaluate as dangerous (Liao et al., 2020). Financial inclusion is being revolutionised by artificial intelligence through the growing use of algorithms to automate risk detection, management, and monitoring (Lopes and Pereira, 2019a). Thanks to the application of artificial intelligence (AI), historically marginalized populations can now access financial services through the use of digital tools like mobile phones or instruments like payment cards that can be used to link with electronic gadgets such as point-of-sale terminals (Alameda 2020). AI gives financial services organizations sophisticated capabilities for risk management and compliance, enabling them to more effectively recognize, evaluate, and reduce risks while abiding by legal obligations. When it comes to identifying anomalies, determining creditworthiness, and keeping an eye on transactions for questionable activity, AI systems perform better than conventional methods.

H4a: *ARMhas significant positive impact on FTS*

H4b: *AI moderate the relationship between ARMand FTS*

Financial Technology and Enhanced Trust: Using AI as Moderator and Handling Security Issues

There has been much discussion and study in recent years on the effects of financial technology on the retail banking industry. According to Fu and Mishra (2022), fintech has made it possible for banks to provide their clients more efficient, flexible, and convenient services through online payment platforms and mobile banking apps, which improve the entire client experience and increase accessibility to financial activities.

However, worries regarding data security and privacy in addition to the effect of competition on service quality have been raised by the emergence of fintech companies and the alternative financial services that they provide (Malaquias and Hwang 2019). The perceived trustworthiness of the supplier has a major effect on acceptance of electronic goods and services from financial institutions by both people as well as businesses (Fu and Mishra, 2022). After the global financial crisis, people's faith in financial organisations—primarily conventional incumbents—was damaged, which caused a shift in favour of fintech (Goldstein et al., 2019). However, users of online banking are exposed to a variety of dangers due to inherent weaknesses in the platform

Citation Information: Sultana, N., Chimote, N.K., Singh, H., Ghani, U., Anwar, M., & Ameen, S. (2025). Securing financial transactions: exploring the role of ai-driven technological influences in enhancing security and trustl. *Academy of Marketing Studies Journal, 29*(4), 1-20.

(Gong et al., 2020), and trust is essential in instances involving risk. Information security elements like confidentiality, authentication, accountability, privacy and permission affect customers' trustworthiness, according to Ashta and Hermann (2021). Accordingly, user-interface design, consumer trust, data security, technical challenges, and a lack of knowledge about the technology all affect the adoption of fintech (Abidin et al., 2019).

Since online banking environments are where the majority of data breaches and identity thefts take place, many clients are cautious and reluctant to transact there because they are worried about the safety of their personal data (Ashta and Hermann, 2021). Fintech companies need to solve privacy and data security issues to raise customer assurance and faith, which will Make sure the wider use Fintech services' adoption and usage (Laksamana et al., 2022). Consequently, Financial service providers, including banks must to disclose more than just their security measures in a clear and concise manner and customer support, but they should also take care of any potential technical issues. Financial service providers, including banks can encourage the growth of e-banking usage by addressing these concerns and building customer trust (Gong et al., 2020).

H5: *FTShas significant positive impact on ENT*

OBJECTIVES

- To assess the moderating artificial intelligence's effects on several financial transaction services, including fraud detection,risk management, transaction monitoring andfurther enhancing financial transaction security measures for better protection and trust

RESEARCH METHODOLOGY

Data Collection, Study Population & Sampling

This research uses a quantitative approach with the goal of determining the causal relationship between the variables. Since consumers of financial transactions services are the organizational figures most likely to have access to the data required for the research, we created a self-administered, online survey for them to complete. The study was carried out by the authors over a period of eight months, from January to August 2024. The surveys were to be completed by the respondents within two weeks of each other. Additionally, the WhatsApp app can be utilised to gather information and get feedback from those working in this industry. In this investigation, 425 samples in total were used. Following sorting, it was discovered that 391 customers provided the sample that was gathered and fully responded to.

Data Analysis

IBM SPSS Statistics v.20 was utilized to evaluate and estimate hypotheses derived from research models. Factor analysis, regression analysis, test hypotheses and Cronbach's alpha were used to determine the validity of the idea statements and the reliability of the suggested model.

Research Instrument

Citation Information: Sultana, N., Chimote, N.K., Singh, H., Ghani, U., Anwar, M., & Ameen, S. (2025). Securing financial transactions: exploring the role of ai-driven technological influences in enhancing security and trustl. *Academy of Marketing Studies Journal, 29*(4), 1-20.

5: Strongly agree; 4: Agree; 3: Disagree; 2: Strongly disagree; 1: were the five Likert paragraphs that were used to build the questionnaire. The earlier literature served as a basis for the questionnaire's development. The survey was separated into three parts: Part A of the report described the respondents' gender, age range, income, experience, and level of education. The questions for every variable and one moderating factor are in Section B. The questionnaire also attempted to gather information as a major source for evaluating the constructs of the model's hypotheses.

Research Variables

The variable that is independent, Enhanced Trust (ENT) which some of the sup can measure variablesFraud Detection and Prevention (FDP); Real-Time Transaction Monitoring (RTM); Automating Risk Management (ARM); Chatbots and Virtual Assistants (CVA) and dependent variable Financial Transaction Security(FTS) Figure 1.

Research Model

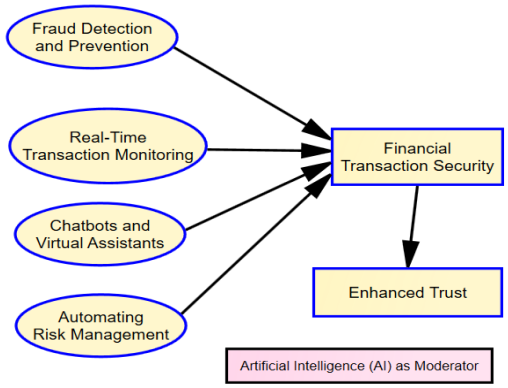

FIGURE 1
RESEARCH MODEL SHOWING THE RELATIONSHIP OF FACTORS INFLUENCING FINANCIAL TRANSACTION SECURITY AND ENHANCED TRUST

RESULTS AND ANALYSIS

Demographic Profile

Descriptive demographic Statistics were employed to assess the respondent's demographic traits. Ultimately, 391 out of 425 questionnaires that were distributed to respondents were found to be completely filled out and error-free. After additional verification, 92% of the responses are deemed to be of good quality. The sociodemographic data for every person is displayed in table. The respondents' gender identity is displayed in Table 1. Out of the 391 responses that were gathered, 326 (83.40%) were from men, while the remaining 65 were from women of 16.6 %.

Further, it displays the responders according to age groups. Out of 391 responders, a total of 108 (27.60 %) The responses are from the age range of 31-40, 96 (24.60 %) the replies come from 51 to 60 age range and about 74 (18.9 %) responses are from 41 to 50 years age group. In the table, which displays the respondents' educational attainment. Work experience and income.

Citation Information: Sultana, N., Chimote, N.K., Singh, H., Ghani, U., Anwar, M., & Ameen, S. (2025). Securing financial transactions: exploring the role of ai-driven technological influences in enhancing security and trustl. *Academy of Marketing Studies Journal, 29*(4), 1-20.

Out of 391 respondents, 159 (40.7%) had professional degrees, 7 to 14 years of work experience and an average salary of roughly 40,000 rupees Table 1.

Table 1
DESCRIPTIVE STATISTICS OF DEMOGRAPHIC PROFILE

		Frequency	Valid %
Gender	Female	65	16.6
	Male	326	83.4
Age profile	21-30 years	51	13
	31-40 years	108	27.6
	41-50 years	74	18.9
	51-60 years	96	24.6
	61 years and above	62	15.9
Highest education level	Undergraduate Degree	50	12.8
	Postgraduate Degree	103	26.3
	Professional Education	159	40.7
	Other	79	20.2
Working experience (in years)	Less than 6	100	25.6
	7 to 14	195	49.9
	15 to 21	78	19.9
	22 to 28	18	4.6
Income	10,000 – 20, 000	85	21.7
	20001 – 30,000	129	33
	30001 – 40,000	143	36.6
	More than 40,000	34	8.7

Exploratory Factor and Reliability Analysis

The EFA was used to determine the significance of the compliant components. The threshold of the experiment is fixed at the factor loading of 0.50 (table 2). These findings imply that factor analysis is an important good method for gathering this data. All elements were those with factor loadings higher than 0.5 considered in the end. A scale is generally regarded as internally consistent if it satisfies the 0.70 Chronbach's Alpha criteria. The Cronbach's alpha level for This inquiry was set at 0.7 (table 2).

Table 2
RESULTS OF EXPLORATORY FACTOR ANALYSIS

Variable	Statement	Factor loadings	KMO Measure of Sample Adequacy (>0.5)	Bartlett's Test of Sphericity		Items confirmed	Items dropped	Cum % of Loading
				Chi Square	Sig. (<.10)			
Fraud Detection and Prevention (FDP)	FRAUD -1	0.143	0.854	2011.935	0.000	4	1	72.875
	FRAUD -2	0.946						
	FRAUD -3	0.955						
	FRAUD -4	0.967						
	FRAUD -5	0.939						
Real-Time Transaction Monitoring (RTM)	TRANS -1	0.903	0.856	1521.764	0.000	5	0	74.404
	TRANS -2	0.922						
	TRANS -3	0.919						
	TRANS -4	0.834						
	TRANS -5	0.717						

Citation Information: Sultana, N., Chimote, N.K., Singh, H., Ghani, U., Anwar, M., & Ameen, S. (2025). Securing financial transactions: exploring the role of ai-driven technological influences in enhancing security and trustl. *Academy of Marketing Studies Journal, 29*(4), 1-20.

Chatbots and Virtual Assistants (CVA)	CHAT -1	0.676	0.710	1013.174	0.000	4	0	70.955
	CHAT -2	0.912						
	CHAT -3	0.949						
	CHAT -4	0.805						
Automating Risk Management (ARM)	RISK -1	0.911	0.866	1578.571	0.000	5	0	75.386
	RISK -2	0.927						
	RISK -3	0.922						
	RISK -4	0.838						
	RISK -5	0.727						
Financial Transaction Security (FTS)	SECURITY -1	0.161	0.849	2038.832	0.000	4	1	72.926
	SECURITY -2	0.949						
	SECURITY -3	0.955						
	SECURITY -4	0.971						
	SECURITY -5	0.930						
Enhanced Trust (ENT)	TRUST -1	0.674	0.728	337.171	0.000	4	1	44.851
	TRUST -2	0.763						
	TRUST -3	0.814						
	TRUST -4	0.116						
	TRUST -5	0.729						
Artificial Intelligence (AI)	AI -1	0.165	0.860	2046.684	0.000	4	1	73.246
	AI -2	0.948						
	AI -3	0.957						
	AI -4	0.968						
	AI -5	0.940						

Table 3
RESULTS OF RELIABILITY ANALYSIS

Variable	Cronbach alpha
Fraud Detection and Prevention (FDP)	0.966
Real-Time Transaction Monitoring (RTM)	0.913
Chatbots and Virtual Assistants (CVA)	0.861
Automating Risk Management (ARM)	0.918
Financial Transaction Security (FTS)	0.966
Enhanced Trust (ENT)	0.736
Artificial Intelligence (AI)	0.967

Normality Test

According to Hair et al. (2022), Skewness measures the degree of symmetry in a variable's distribution. If the distribution leans, it is skewed towards either the tail on the left or the tail on the right. More Positive skewness indicates more little numbers, while negative skewness indicates larger values. Skewness numbers between -1 and +1 are exceptional, although those between -2 and +2 are usually acceptable. Values over -2 and +2 indicate significant non-normality. Similarly, Kurtosis indicates whether the distribution is normal when contrasted to one that is overly peaked or flat. A distribution with positive kurtosis is more peaked, while a negative kurtosis person is flatter. Kurtosis greater than +2 indicates an overly peaked distribution, while kurtosis less than -2 indicates an overly flat distribution. A distribution that is typical is one in which skewness and kurtosis are near zero. As seen in table 3, the descriptive data for all the variables show, with the exception of ENT, a comparatively symmetrical distribution with mild tails, with a negligible skewness of 0.5 and a kurtosis of -0.2.

Citation Information: Sultana, N., Chimote, N.K., Singh, H., Ghani, U., Anwar, M., & Ameen, S. (2025). Securing financial transactions: exploring the role of ai-driven technological influences in enhancing security and trustl. *Academy of Marketing Studies Journal, 29*(4), 1-20.

All of the results point to the data being roughly normally distributed, which supports the validity of parametric statistics. l analysis applied to these variables in subsequent analysis.

Table 4
RESULTS OF NORMALITY TEST

Variables	Skewness	Kurtosis
Fraud Detection and Prevention (FDP)	0.555	-0.184
Real-Time Transaction Monitoring (RTM)	0.524	-0.113
Chatbots and Virtual Assistants (CVA)	0.337	-0.682
Automating Risk Management (ARM)	0.501	-0.200
Financial Transaction Security (FTS)	0.546	-0.226
Enhanced Trust (ENT)	0.347	0.603
Artificial Intelligence (AI)	0.485	-0.330

Correlation Analysis

The outcomes of the independent variable analysis of correlation suggest that every variable appears to have a significant association with the others. When all factors are considered, there is an substantial correlation between the independent and dependent variables (Table 4). The variables evaluating FDP and FTS had the highest level of correlation (0.997), while those measuring CVA and ENT had the least significant link (0.725).

Table 5
CORRELATIONS

		FDP	RTM	CVA	ARM	FTS	ENT	AI
FDP		1						
RTM		.943**	1					
CVA		.917**	.885**	1				
ARM		.944**	.987**	.899**	1			
FTS		.997**	.938**	.919**	.949**	1		
ENT		.815**	.788**	.751**	.803**	.821**	1	
AI		.988**	.922**	.912**	.929**	.987**	.838**	1

**. Correlation is significant at the 0.01 level (2-tailed).

Regression Analysis

The connection between the independent and dependent variables was determined using stepwise regression analysis. The study's main goals were to evaluate the moderating consequences of AI-powered technology on Securing Financial Transactions and thus enhancing Security and Trust.

Financial Transaction Security (FTS) as Dependent Variable

Stepwise analysis of the regression was accustomed to ascertain the predictor-criterion connection between the independent and dependent factors. Using step-by-step regression analysis, Tables 5-15 demonstrated that the factors under examination are highly significant

Citation Information: Sultana, N., Chimote, N.K., Singh, H., Ghani, U., Anwar, M., & Ameen, S. (2025). Securing financial transactions: exploring the role of ai-driven technological influences in enhancing security and trustl. *Academy of Marketing Studies Journal, 29*(4), 1-20.

predictors of the FTS shows that these features account for 99.80% of FTS, with R square of 0.998 shows the ANOVA values for the regression model, which show 95% confidence level validation. The beta value of 0.978, which accurately reflects their influence on FTS, is shown in the summary of coefficients.

Table 6
REGRESSION ANALYSIS

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.999[a]	.998	.998	.04169
a. Predictors: (Constant), CVA, RTM, FDP, ARM				

Table 7
ANOVA ANALYSIS

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	395.881	4	98.970	56937.135	.000[b]
	Residual	.671	386	.002		
	Total	396.551	390			
a. Dependent Variable: FTS						
b. Predictors: (Constant), CVA, RTM, FDP, ARM						

Table 8
REGRESSION COEFFICIENTS TABLE FOR DEPENDENT VARIABLES

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.000	.007		-.068	.946
	FDP	.983	.008	.979	130.719	.000
	ARM	-.403	.015	-.358	-26.904	.000
	CVA	-.004	.006	-.004	-.714	.475
	RTM	.425	.015	.382	27.798	.000
a. Dependent Variable: FTS						

Moderating Impact of Artificial intelligence (AI) between Selected Influencing Variables and Financial Transaction Security (FTS)

Zscore values were generated for every variable in order to examine the link between them. The interaction between all independent elements and AI is then computed to create new variables, which are referred to as interactions IA1 through IA4.

FTS was the dependent variable, and IA1 through IA4, the extra interacting independent variables, were used in a regression analysis. The FTS can be strongly predicted by the interacting features, as shown, which show the outcomes of step-wise regression analysis. These factors account for 88% of the FTS, as indicated by Table 6 R square value of 0.880. The ANOVA data in Table 6 indicate the regression model's validation at a 95% degree of certainty. According to The summary of the coefficient displayed in Table 6, the beta values are, respectively, 0.839 and 0.350. The way these concepts impact the FTS is accurately depicted by them.

Table 9
Regression analysis

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate

Citation Information: Sultana, N., Chimote, N.K., Singh, H., Ghani, U., Anwar, M., & Ameen, S. (2025). Securing financial transactions: exploring the role of ai-driven technological influences in enhancing security and trustl. *Academy of Marketing Studies Journal, 29*(4), 1-20.

1	.938[a]	.880	.879	.35100
a. Predictors: (Constant), IA4, IA3, IA1, IA2				

Table 10
ANOVA ANALYSIS

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	348.996	4	87.249	708.181	.000[b]
	Residual	47.556	386	.123		
	Total	396.551	390			
a. Dependent Variable: FTS						
b. Predictors: (Constant), IA4, IA3, IA1, IA2						

Table 11
REGRESSION COEFFICIENTS TABLE FOR DEPENDENT VARIABLES

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.528	.018		137.085	.000
	IA1	.237	.020	.839	11.842	.000
	IA2	-.091	.029	-.320	-3.148	.002
	IA3	.021	.016	.071	1.357	.176
	IA4	.100	.030	.350	3.302	.001
a. Dependent Variable: FTS						

Impact of Financial Transaction Security (FTS) on Enhanced Trust (ENT)

Stepwise regression analysis was used to find the predictor-criterion relationship between the independent and dependent variables. The ENT is significantly predicted by FTS, as tables 7 and 7 show. These factors account for 67.30% of the ENT, as Table 7 shows (R square: 0.673). A 95% confidence level of validation is shown by the regression model's ANOVA results, which are displayed in Table 7. The beta value of the component is 0.821, which accurately reflects their influence, The summary of the coefficient indicates in Table 7.

Table 12
REGRESSION ANALYSIS

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.821[a]	.673	.672	.44322
a. Predictors: (Constant), FTS				

Table 13
ANOVA ANALYSIS

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	157.442	1	157.442	801.473	.000[b]
	Residual	76.415	389	.196		
	Total	233.857	390			
a. Dependent Variable: ENT						
b. Predictors: (Constant), FTS						

Citation Information: Sultana, N., Chimote, N.K., Singh, H., Ghani, U., Anwar, M., & Ameen, S. (2025). Securing financial transactions: exploring the role of ai-driven technological influences in enhancing security and trustl. *Academy of Marketing Studies Journal, 29*(4), 1-20.

Table 14
REGRESSION COEFFICIENTS TABLE FOR DEPENDENT VARIABLES

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.171	.066		17.714	.000
	SECURITY	.630	.022	.821	28.310	.000
a. Dependent Variable: ENT						

Results of Hypotheses Testing

Table 15 lists the 5 initial hypotheses put forth by the conceptualresearch framework, of which 4 have been accepted and the remaining 1, hypothesis 3a and 3b are rejected.

Table 15
SUMMARY OF HYPOTHESES TESTING

Hy. No.	IndependentVariables	Dependent Variables	R-Square	Beta Coefficient	t-value	Sig Value	Status of Hypotheses
H1a	FDP	FTS	0.998	0.979	130.719	0.000	Accepted
H2a	RTM			-0.358	-26.904	0.000	Accepted
H3a	CVA			-0.004	-0.714	0.475	Rejected
H4a	ARM			0.382	27.798	0.000	Accepted
H1b	IA1 (ZFDP*AI)	FTS	0.880	0.839	11.842	0.000	Accepted
H2b	IA2 (ZRTM*AI)			-0.320	-3.148	0.002	Accepted
H3b	IA3 (ZCVA*AI)			0.071	1.357	0.176	Rejected
H4b	IA4(ZARM*AI)			0.350	3.302	0.001	Accepted
H5	FTS	ENT	0.673	0.821	28.310	0.000	Accepted

Discussion

Fraud Detection and Prevention (FDP) and Financial Transaction Security (FTS)were found to be significantly positively correlated with Artificial intelligence (AI) (H1a and H1b; beta coefficient =0.979 and 0.839). AI algorithms, according to Shoetan&Familoni (2024), provide sophisticated capabilities for identity verification and authentication, allowing businesses to precisely confirm the identities of their clients and identify attempts at unlawful access (Adekanmbi and Wolf, 2024). AI-driven identity verification systems examine a many identity documents, including passports, cards of identification issued by the government and biometric information like Facial recognition and fingerprints, using learning by machine techniques, natural language processing and biometric authentication. These technological advancements, according to Pomerleau & Lowery (2020), can authenticate identification documents and identify attempts by fraudsters to pose as genuine users (Jakubiec, 2020). Additionally, by examining user conduct and interaction patterns, AI systems are able to create a baseline for normal behavior. Any deviations from this baseline can set off alerts for possible fraudulent activity, allowing financial institutions to take action and stop unauthorized access to sensitive data or

Citation Information: Sultana, N., Chimote, N.K., Singh, H., Ghani, U., Anwar, M., & Ameen, S. (2025). Securing financial transactions: exploring the role of ai-driven technological influences in enhancing security and trustl. *Academy of Marketing Studies Journal, 29*(4), 1-20.

accounts. AI provides advanced instruments to identify and counteract deceptive practices instantly by utilizing data analytics, Predictive modelling as well as machine learning (Devan et al., 2023, Hassan et al., 2023).

The empirical analysis of hypotheses 2a and 2b revealed a substantial negative correlation between Real-Time Transaction Monitoring (RTM)and Financial Transaction Security (FTS) (beta coefficient = -0.358 and -0.320),with Artificial intelligence (AI), acting as a moderating factor. Rahmani et al. (2023) assert that AI analytics provide financial institutions the capacity to automate regulatory compliance procedures like know-your-customer due diligence, anti-money laundering monitoring, and reporting of suspicious activity. Such systems can Analyse transactional patterns, customer data, and external data sources to find potential compliance risks and guarantee that regulations are followed. According to Dahal (2023), financial organisations are able to effectively mitigate regulatory risks, improve their risk management capabilities, and streamline compliance operations by utilizing AI analytics. According to Girija et al. (2023), companies may enhance transparency and security throughout the entire financial system through the integration of blockchain transactional networks with fraud detection systems driven by AI. These systems examine vast volumes of transactional data and identify anomalies that might indicate fraud using machine learning techniques (Tyagi et al., 2020). Block chain technology offers a safe and impermeable platform for storing and confirming transactions, guaranteeing the accuracy and exchangeability of transaction records. Transactional data is analyzed by real-time AI algorithms to look for trends, abnormalities, and unusual activities that could be signs of fraud. The blockchain enables the recording of fraud alarms, resulting in an auditable record of fraudulent conduct and enabling timely risk mitigation steps (Kumar et al., 2023). Furthermore, the transparency of blockchain allows all network users to view and validate transaction histories, which promotes increased responsibility and confidence. Organizations may build a more robust and secure financial ecosystem that guards against fraud, manipulation, and unauthorized actions by fusing block chain fraud detection using AI-powered transactional networks (Rane et al., 2023). In the era of digitalisation, where identity Both account takeover and theft are common dangers, identity verification is an essential component of financial transaction security (Sehgar and Zukarnain, 2021).

An independent study of the relationship between Chatbots and Virtual Assistants (CVA) and Financial Transaction Security (FTS) found no significant correlation between the two concepts. Hypothesis 3a (p =0.475) is not supported by the results, not even under the influence of AI (H3b, p =0.176). Although AI is based on the creation of a program for data quality, the use of clever robots carries a danger of liability (Harkut and Kasat 2019). Sometimes banks are reluctant to give computers total autonomy because of the erratic behavior that they exhibit. They frequently decide to have a human supervisor on staff when making critical machine decisions, such blocking or releasing funds (Mhlanga, 2020). This somewhat disproves the fundamental rationale for using virtual assistants and chatbots. Regulations, corporate culture, and very strict operational security and compliance standards can all serve as obstacles to the broad application of artificial intelligence in banking organizations. A barrier may also be In sufficient awareness of the dangers connected to AI.

Significant findings (hypotheses 4a and 4b) indicate that when combined with Artificial intelligence (AI), Automating Risk Management (ARM) does, in fact, significantly increase Financial Transaction Security (FTS) (beta coefficient = 0.382 and 0.350). As per Ray et al. (2019), AI is necessary to lower currency risk and simplifying risk management. While the dollar is the most common car money used in deals, a lot of clients are adopting bitcoin as their vehicle

Citation Information: Sultana, N., Chimote, N.K., Singh, H., Ghani, U., Anwar, M., & Ameen, S. (2025). Securing financial transactions: exploring the role of ai-driven technological influences in enhancing security and trustl. *Academy of Marketing Studies Journal, 29*(4), 1-20.

currency. People and small businesses can choose to add money using fiat money through digital finance, shifting the financial intermediary's risk of volatility (Chang et al., 2020). With block chain platforms and bitcoin acting as a medium of exchange, the volatility of virtual money is eliminated for both the sender and the recipient. Small income earners can now participate in the financial sector due to AI technology's strength in risk prevention (Alameda 2020). To put it briefly, financial professionals are using AI-powered models that are more exciting and nimble as the financial markets accept it more and more. These models are used to identify risks, identify trends, save labor, assure better information, and prepare for the future (Bouchama & Kamal, 2021). According to Kunduru (2023), AI analytics provide useful tools for risk management and regulatory compliance. These tools help firms recognize, evaluate, and reduce risks in an efficient manner while maintaining compliance with legal standards.

After hypotheses 5 were empirically explored, a significant positive relationship between Financial Transaction Security (FTS) andEnhanced Trust (ENT)was discovered (beta coefficient =0.821). faith is essential in the digital age, especially faith in digital platforms, technology, and institutions—a concept known as "digital trust." Users' confidence in the capacity of electronic organizations, businesses, technologies, as well as procedures to establish a secure digital environment by protecting users' privacy about their personal information is known as digital trust (Jelovac et al., 2021). Trust in digital systems is linked to confidence in digital platforms, technologies, and institutions. In order to create and preserve digital trust, modern enterprises and organizations must embrace an AI culture. Fintech companies stand to benefit greatly from this, such as the ability to shape their own futures, build and maintain enduring relationships with stakeholders, enhance their standing, acquire a competitive advantage, and boost productivity and employee cohesion (Herden et al., 2021).

In the digital banking sector, it is essential to safeguard individuals' private data by adhering to data-privacy rules and regulations (Ayaburi, 2022). Companies must take the required precautions to secure personal information and get individuals' express consent before processing their data in certain situations. To maintain compliance with data protection laws and regulations, fintech companies must adopt numerous security measures to stop violations of data privacy. The previously indicated actions include the execution between secure authentication and encryption procedures, de-identification methods, recurring assessments, and the development of regulations pertaining to protection of data (Beg et al., 2022). The governance of data frameworks, which define roles and duties, data-handling techniques, and compliance procedures, can guarantee moral and responsible big-data management. According to Abdin et al. (2019), regular audits, staff instruction on data security, and protocols for locating and resolving privacy issues are also necessary. Thorough data analysis and machine learning that protects privacy algorithms are necessary when deploying AI systems to prevent confusing Prejudice and unauthorised access to private information (Abed and Anupam, 2022).

CONCLUSION

In conclusion, integrating AI presents a ground-breaking chance to enhance security protocols in the monetary services sector. Through incorporating AI algorithms and The unchangeable ledger of block-chain technology, enterprises may generate inventive resolutions that efficiently tackle diverse security issues. The potential for enhancing security and trust in financial transactions with AI integration is substantial. The safe and transparent platform of block chain, along Using AI-powered identity verification, fraud detection, and smart contract automation, improve security protocols, lower risks, and promote confidence inside the financial

Citation Information: Sultana, N., Chimote, N.K., Singh, H., Ghani, U., Anwar, M., & Ameen, S. (2025). Securing financial transactions: exploring the role of ai-driven technological influences in enhancing security and trustl. *Academy of Marketing Studies Journal, 29*(4), 1-20.

industry. The study also offers best practices as well as approaches that fintech organizations can use to guarantee privacy and data security. The implications of these findings should be taken into consideration by legislators, financial institutions, & more parties involved that wish to guarantee the moral and responsible use of AI in the field of digital finance.

Future Prospects

Deep learning Two instances of this are reinforcement learning and advanced AI algorithms whose further study can improve the capabilities of financial services powered by AI security solutions. These algorithms can discover new dangers, increase the accuracy of fraud detection, and give users more individualized security precautions. In relation to integrating blockchain technology and artificial intelligence, a study of techniques that protect privacy such as Homomorphic encryption and zero-knowledge proofs can help ease concerns about data security and privacy. These methods improve trust and confidence in financial transactions by enabling the secure calculation and analysis of sensitive data without compromising privacy. Blockchain network scalability and interoperability innovations can enable smooth integration with AI-driven apps and other financial systems. The effectiveness and scalability of blockchain-based security solutions can be increased through research into compatible blockchain protocols and scalability techniques like sidechains and sharding.

This study clarified how privacy issues in the fintech sector interact with artificial intelligence and offered suggestions for improving data security and protection. However, a number of topics require more research to improve our comprehension Among the moral dilemmas in fintech. Future research should concentrate on addressing privacy and data security concerns in relation to the complex relationship between fintech and customer confidence. Second, studies on how to foster trust in the age of fintech—like corporate digital responsibility or observing Rules and rules pertaining to data protection —might be conducted. Future studies on the influence of social and cultural norms on fintech adoption and the application of big data artificial intelligence in the banking industry may also prove to be fascinating.

LIMITATIONS

Although this study has limitations, it offers insightful information about AI's impact on cybersecurity. It takes a broad view of how Cyber-AI would affect consumers, neglecting the variations in organization types, sizes, industries, and locales, all of which may have different outcomes. It doesn't go into specific AI technology in detail, which restricts our understanding of the whole range of implications. Owing to temporal limitations, the literature search was restricted to four databases, potentially omitting relevant content from additional sources. Furthermore, the selection of relevant literature was made more narrowly by the inclusion/exclusion criteria. To further delve into the results, it is imperative to discuss the study's shortcomings and the requirement for further resources. Through the acquisition of more extensive data and the extension of current understanding, researchers will be better equipped to comprehend the intricate ethical and privacy concerns related to fintech.

REFERENCES

Abdel-Rahman, M. (2023). Advanced cybersecurity measures in IT service operations and their crucial role in safeguarding enterprise data in a connected world. *Eigenpub Reviewof Science and Technology, 7*(1), 138-158.

Citation Information: Sultana, N., Chimote, N.K., Singh, H., Ghani, U., Anwar, M., & Ameen, S. (2025). Securing financial transactions: exploring the role of ai-driven technological influences in enhancing security and trustl. *Academy of Marketing Studies Journal, 29*(4), 1-20.

Abed, A. K. and Anupam, A. (2022). Review of security issues in Internet of Things and artificial intelligence-driven solutions. *Security and Privacy* 6(3): e285.

Abidin, M. A. Z., Anuar, N. and Salin, A. S. A. P. (2019). Customer data security and theft: A Malaysian organization's experience. *Information and Computer Security*, 27(1): 81–100.

Adekanmbi, A.O. & Wolf, D. (2024). Solid Mineral Resources Extraction and Processing Using Innovative Technology in Nigeria. *ATBU Journal of Science, Technology andEducation*, *12*(1), 1-16.

Alam, S.S., Ali, M.H., Omar, N. A. and Hussain, W.M.H. W. (2020). "Customer satisfaction in online shopping in growing markets: An empirical study," *Int. J. Asian Bus. Inf. Manag.*, 11(1):78– 91.

Alameda, T. (2020). Data, AI and financial inclusion: the future of global banking—Responsible Finance Forum, BBVA 2020.

Ashta, A. and Herrmann, H. (2021). Artificial intelligence and fintech: An overview of opportunities and risks for banking, investments, and microfinance. *Strategic Change*, 30(3): 211–22.

Ayaburi, E. W. (2022). Understanding online information disclosure: Examination of data breach victimization experience effect. *Information Technology and People*, 36(1): 95–114.

Beg, S., Khan, S.U.R. and Anjum, A. (2022). Data usage-based privacy and security issues in mobile app recommendation (MAR): A systematic literature review. *Library Hi Tech*, 40: 725–49.

Bouchama, F. & Kamal, M. (2021). Enhancing cyber threat detection through machine learning-based behavioralmodeling of network traffic patterns. *International Journalof Business Intelligence and Big Data Analytics*, *4*(9), 1-9.

Chahal, S. (2023). Navigating Financial Evolution: Business process optimization and digital transformation in the finance sector. *International Journal of Finance*, *8*(5), 67-81.

Chang, V., Baudier, P., Zhang, H., Xu, Q., Zhang, J. & Arami, M. (2020). How Blockchain can impact financial services–The overview, challenges and recommendations from expert interviewees. *Technological Forecasting and Social Change*, *158*, 120166.

Dahal, S. B. (2023). Utilizing Generative AI for Real-Time financial market analysis opportunities and challenges. *Advances in Intelligent Information Systems*, *8*(4), 1-11.

Daníelsson, J., Macrae, R. and Uthemann, A. (2022). Artificial intelligence and systemic risk. *Journal of Banking and Finance*, 140: 106290.

Devan, M., Prakash, S. &Jangoan, S. (2023). Predictive maintenance in banking: leveraging AI for real-time data analytics. *Journal of Knowledge Learning and Science Technology*, *2*(2), 483-490.

Duy Phuong, N.N., Luan, L. T., Van Dong, V. and Le Nhat Khanh, N. (2020). Examining customers' continuance intentions towards e-wallet usage: The emergence of mobile payment acceptance in Vietnam.*J. Asian Financ. Econ. Bus.*, 7(9), 505–516.

Frank, M. R. (2019). The Evolution of AI Research and the Study of Its Social Implications. MIT MEDIA LAB 2019.

Fu, J. and Mishra, M. (2022). Fintech in the time of COVID-19: Technological adoption during crises. *Journal of Financial Intermediation*, 50: 100945.

Girija, D. K., Rashmi, M., William, P. & Yogeesh, N. (2023). Framework for integrating the synergies of blockchain with AI and IoT for secure distributed systems. In International Conference on Data Analytics and Insights (pp. 257-267). Singapore: *Springer Nature Singapore*.

Goldstein, I., Jiang, W. and Karolyi, G. A. (2019). To FinTech and beyond. *The Review of Financial Studies*, 32(5): 1647–61.

Gong, X., Zhang, K.Z.K., Chen, C., Cheung, C.M.K. and Lee, M.K.O. (2020). What drives trust transfer from web to mobile payment services? The dual effects of perceived entitativity. *Information & Management*, 57(7): 103250.

Hair, J. F., Hult, G. T. M., Ringle, C. M. & Sarstedt, M. (2022). A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM) (3 ed.). Thousand Oaks, CA: Sage.

Harkut, D. G. and Kasat, K. (2019). Introductory Chapter: Artificial Intelligence—Challenges and Applications. In Artificial Intelligence—Scope and Limitations. London: Intech Open.

Hassan, M., Aziz, L. A. R. &Andriansyah, Y. (2023). The role artificial intelligence in modern banking: an exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. *Reviews of Contemporary Business Analytics*, *6*(1), 110-132.

Hassani, H., Silva, E. S., Unger, S., TajMazinani, M. and Feely, S.M. (2020). Artificial Intelligence (AI) or Intelligence Augmentation (IA): What Is the Future? *AI*, 1(2): 143–55.

Herden, C. J., Alliu, E., Cakici, A., Cormier, T., Deguelle, C., Gambhir, S. and et al. (2021). Corporate Digital Responsibility. *Nachhaltigkeits Management Forum*, 29: 13–29.

Citation Information: Sultana, N., Chimote, N.K., Singh, H., Ghani, U., Anwar, M., & Ameen, S. (2025). Securing financial transactions: exploring the role of ai-driven technological influences in enhancing security and trustl. *Academy of Marketing Studies Journal, 29*(4), 1-20.

Irshad. & Neha (2013), "A study on impact of e-banking awareness on customers' attitude towards its use" International Journal of Marketing & Financial Management, Vol. 1, Issue 1, Dec-2013, pp 01-23.

Jakubiec, W. (2020). Threats of identity theft in cyberspace-case study. *ASEJ Scientific Journal of Bielsko-Biala School of Finance and Law*, 24(2), 10-14.

Jelovac, D., Ljubojevic´, C. and Ljubojevic´, L. (2021). HPC in business: The impact of corporate digital responsibility on building digital trust and responsible corporate digital governance. *Digital Policy, Regulation and Governance* 24(6): 485–497.

Kafi, M. A. & Akter, N. (2023). Securing financial information in the digital realm: case studies in cybersecurity for accounting data protection. *American Journal of Trade andPolicy*, *10*(1), 15-26.

Kavitha, B. and Rajini, G. (2024). The Impact of AI-driven Technological Influences on Security Measures within Digital Wallets amid Digital Revolution.*International Journal of Intelligent Systems and Applications in Engineering*, 12(12s), 259–265.

Kumar, S., Lim, W. M., Sivarajah, U. & Kaur, J. (2023). Artificial intelligence and blockchain integration in business: trends from a bibliometric-content analysis. *InformationSystems Frontiers*, *25*(2), 871-896.

Kunduru, A. R. (2023). Artificial intelligence advantages in cloud Fintech application security. *Central Asian Journal of Mathematical Theory and Computer Sciences*, *4*(8), 48-53.

La Torre, M., Botes, V. L., Dumay, J. and Odendaal, E. (2019). Protecting a new Achilles heel: The role of auditors within the practice of data protection. *Managerial Auditing Journal* 36: 218–39. DOI 10.1108/MAJ-03-2018-1836

Lai, P. C. & Tong, D. L. (2022). An Artificial Intelligence-Based Approach to Model User Behavior on the Adoption of E-Payment. In Handbook of Research on Social Impacts of E-Payment and Blockchain Technology (pp. 1-15). IGI Global.

Laksamana, P., Suharyanto, S. and Cahaya, Y. F. (2022). Determining factors of continuance intention in mobile payment: Fintech industry perspective. *Asia Pacific Journal of Marketing and Logistics*, 35(1).

Liao, G., Yao, D. and Hu, Z. (2020). The Spatial Effect of the Effciency of Regional Financial Resource Allocation from the Perspective of Internet Finance: Evidence from Chinese Provinces. *Emerging Markets Finance and Trade*, 56(6): 1211–1223.

Liyanaarachchi, G., Deshpande, S. and Weaven, S. (2020). Market-oriented corporate digital responsibility to manage data vulnerability in online banking. *International Journal of Bank Marketing* 39(4): 571–91.

Lopes, J. and Pereira, J. L. (2019b). Blockchain technologies: Opportunities in healthcare. In Advances in Intelligent Systems and Computing. Cham: *Springer*, pp. 435–42.

Lopes, J., and Pereira, J.L. (2019a). Blockchain projects ecosystem: A review of current technical and legal challenges. In Advances in Intelligent Systems and Computing. Cham: *Springer,* pp. 83–92.

Malaquias, R. F. and Hwang, Y. (2019). Mobile banking use: A comparative study with Brazilian and US participants. *International Journal of Information Management* 44: 132–40.

Mangla D and Parkar B. (2021), "A study on Calculating, risk, return and proportion of each security in the portfolio diversification", International Journal of Social Sciences & Economic Environment, Vol. 6,Issue 1, Jan-Jun-2021, pp 08–14.

Mhlanga, D. (2020). Industry 4.0 in Finance: The Impact of Artificial Intelligence (AI) on Digital Financial Inclusion.*Int. J. Financial Stud.*, 8: 45.

Nasr, M. H., Farrag, M. H. & Nasr, M. (2020). E-payment systems risks, opportunities, and challenges for improved results in e-business. *International Journal of Intelligent Computing and Information Sciences*, 20(1), 16-27.

Nzuva, S. (2019). Smart contracts implementation, applications, benefits, and limitations. *Journal of Information Engineering and Applications*, *9*(5), 63-75.

Olweny, F. (2024). Navigating the nexus of security and privacy in modern financial technologies. *GSC Advanced Research and Reviews*, *18*(2), 167-197.

Pomerleau, P. L. & Lowery, D. L. (2020). Countering cyber threats to financial institutions. In a private and public partnership approach to critical infrastructure protection. *Springer.*

Rahmani, A. M., Rezazadeh, B., Haghparast, M., Chang, W. C., & Ting, S. G. (2023). Applications of artificial intelligence in the economy, including applications in stock trading, market analysis, and risk management. *IEEE Access*, *11*.

Rakha, N. A. (2023). Navigating the legal landscape: corporate governance and anti-corruption compliance in the digital age. *International Journal of Management and Finance*, *1*(3).

Rane, N., Choudhary, S. P. & Rane, J. (2023). Blockchain and Artificial Intelligence (AI) integration for revolutionizing security and transparency in finance.

Citation Information: Sultana, N., Chimote, N.K., Singh, H., Ghani, U., Anwar, M., & Ameen, S. (2025). Securing financial transactions: exploring the role of ai-driven technological influences in enhancing security and trustl. *Academy of Marketing Studies Journal, 29*(4), 1-20.

Ray, S., Paul, S. and Miglani, S. (2019). Use of Blockchain and Artificial Intelligence to Promote Financial Inclusion in India. *TECH MONITOR*,1.

Reim,W., Åström, J. and Eriksson, O. (2020). Implementation of Artificial Intelligence (AI): A Roadmap for Business Model Innovation. *AI*, 1(2): 180–191.

Saltz, J. S. and Dewar, N. (2019). Data science ethical considerations: A systematic literature review and proposed project framework. *Ethics and Information Technology*, 21(5): 197–208.

Shinde, N. K., Seth, A. & Kadam, P. (2023). Exploring the Synergies: A Comprehensive Survey of Blockchain Integration with Artificial Intelligence, Machine Learning, and IoT for Diverse Applications. In chapter: Machine Learning and Optimization for Engineering Design, pp 85-119.

Shoetan, P. O. &Familoni, B. T. (2024). Transforming fintech fraud detection with advanced artificial intelligence algorithms. *Finance & Accounting Research Journal*, *6*(4):602-625.

Smith, J. & Liu, C. (2024). *Secure Transactions, Secure Systems: Regulatory Compliance in Internet Banking* (No. 12318). Easy Chair.

Świątkowska, J. (2020). Tackling cybercrime to unleash developing countries' digital potential. *Pathways for Prosperity Commission Background Paper Series*, *33*, 2020-01.

Thakur, M. (2024). Cyber security threats and countermeasures in digital age. *Journal of Applied Science and Education (JASE)*, *4*(1), 1-20.

Tyagi, A. K., Aswathy, S. U. and Abraham, A. (2020). Integrating Blockchain Technology and Artificial Intelligence: Synergies, Perspectives, Challenges and Research Directions. *Journal of Information Assurance and Security*, 15 (5) pp. 178-193.

Vannucci, V. and Pantano, E. (2020). Do I Lose my Privacy for a Better Service? Investigating the Interplay between Big Data Analytics and Privacy Loss from Young Consumers' Perspective. In Retail Futures. Bingley: Emerald Publishing Limited, pp. 193–205.

Wang, X. and He, G. (2020). Digital financial inclusion and farmers' vulnerability to poverty: Evidence from rural China. *Sustainability*, 12(4): 1668.

Yang, J., Zhao, Y., Han, C., Liu, Y. and Yang, M. (2022). Big data, big challenges: Risk management of financial market in the digital economy. *Journal of Enterprise Information Management* 35: 1288–304.

Yu, T. R. and Song, X. (2021). Big Data and Artificial Intelligence in the Banking Industry. In Handbook of Financial Econometrics, Mathematics, Statistics, and Machine Learning, chapter 117, pp. 4025-4041. World Scientific Publishing Co. Pte. Ltd.

Received: 05-Mar-2025, Manuscript No. AMSJ-25-15737; **Editor assigned:** 06-Mar-2025, PreQC No. AMSJ-25-15737(PQ); **Reviewed:** 28-Mar-2025, QC No. AMSJ-25-15737; **Revised:** 22-Apr-2025, Manuscript No. AMSJ-25-15737(R); **Published:** 02-May-2025

Citation Information: Sultana, N., Chimote, N.K., Singh, H., Ghani, U., Anwar, M., & Ameen, S. (2025). Securing financial transactions: exploring the role of ai-driven technological influences in enhancing security and trustl. *Academy of Marketing Studies Journal, 29*(4), 1-20.