Journal of International Commercial Law and Technology
Print ISSN: 1901-8401

Website: https://www.jiclt.com

Article

"Investigating E-Banking And E-Fraud: A Cross-Sectional Study With Demographic Insights In Himachal Pradesh"

Article History:

Name of Author
Dr. Rajat Sharma[1*], Dr. Akhil Sharma[2], Vipul Sharma[3]

Affiliation
[1]Assistant Professor Department of Commerce and Management Career Point University, Hamirpur
[2]Assistant Professor Department of Commerce School of Commerce and Management Studies Central University of Himachal Pradesh, Dharamshala
[3]Research Scholar School of Commerce and Management Studies Central University of Himachal Pradesh, Dharamshala

How to cite this article: Dr. Rajat Sharma, Dr. Akhil Sharma, Vipul Sharma, "Investigating E-Banking And E-Fraud: A Cross-Sectional Study With Demographic Insights In Himachal Pradesh" *J Int Commer Law Technol.* 2026;7(1): 20-31

©2025 the Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License http://creativecommons.org/licenses/by/4.

Abstract
This research examines the relationship between e-banking payments and e-fraud in Himachal Pradesh, focusing on the districts of Kangra, Mandi, and Shimla. The study, conducted between July and September 2023, utilises a cross-sectional design and a primary data collection method involving 357 respondents. The data is collected through self-administered questionnaire from 357 respondents. Exploratory and confirmatory factor analyses, independent sample t-tests, ANOVA, and correlation techniques were employed for data analysis and scale purification. The findings indicate that demographic factors such as gender, occupation, and educational qualification do not significantly influence e-payments. Additionally, the research reveals a weak but significant relationship between e-payments and e-frauds, attributed to the state's high literacy rate, banking initiatives, and enhanced security measures. However, several limitations need to be considered when interpreting the results. Firstly, the selection of districts based solely on population statistics may introduce bias, as it overlooks districts with differing socio-economic characteristics. Secondly, the subjectivity in screening questionnaire responses and disparities in response rates between online and offline distribution methods may affect the reliability of the findings. Moreover, the study's limited inclusion of demographic variables suggests the need for incorporating additional factors to gain a more comprehensive understanding of e-payment adoption trends and potential disparities across socio-economic groups[1].

Keywords: E-banking payments, e-fraud, Himachal Pradesh, cross-sectional study, demographic factors.

Introduction:
Advancements in technology in the 1990s and frequent use of online trade and business have given rise to fast transactions. This sudden upgradation in technology and instant growth in internet usage has also opened the doors for an effortless way to bulky transactions and numerous electronic payment systems. Surely, it was great to align technology with the transaction, but this system also brings out the problem of fraud in electronic payments (Fernandes, 2013). A study from *Javelin Strategy and Research* found that there are about 14.4 million victims are present of e-payments globally in 2018, which is thrice that of 2016. *Juniper Exploration 2016* calculated that the overall cost to the banking system through cybercrime would be around 2.1 trillion in 2019 (Rao, 2019). Financial costs in terms of fraud are one of the major problems with which banks are dealing throughout the world. Fraud is surely unethical, immoral, and unlawful. There are various measures have been taken by banks to prevent these frauds, but they are still not enough (Gee and Button, 2019). 71 per cent of consumers are more concerned about their security numbers during online transactions, followed by convenience at 20 per cent, and after that, personalisation at 9 per cent. Simultaneously, in the Asia-Pacific region, data revealed in a report by

[1] *USE OF ARTIFICIAL INTELLIGENCE IN SUPREME COURT*, (2025), https://www.pib.gov.in/PressReleseDetail.aspx?PRID=2148356.

Experian Identity 2019. Look anywhere in the world, the results related to online banking fraud are the same, whether in America, the Middle East, or the Asia Pacific region. Cyber and Data Breaches are at the top of banking fraud, followed by faster payment options, and social engineering is at third (Global Banking Fraud Survey, 2019).

In the Indian context, it was the Indian Contract act, of 1872 that defines general fraud first time in section 17 but the definition of bank fraud was given by Bhagwan Das Narang who conducted a large-scale survey on bank fraud and defines it as the "*deliberate act of omission or commission by any person carried out in the course of banking transaction or the books of accounts maintained manually or under computer system in banks, resulting in the wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank"* (Mohan, 2000). To have consistency in reportage, scams have been classified, based mainly on the requirements of the Indian Penal Code: 1. Misuse and criminal breach of trust. 2. Deceitful encashment through forged instruments, manipulation of books of account or through fabricated accounts, and conversion of property. 3. Unauthorised credit facilities extended for recompense or illegal fulfilment. 4. Carelessness and cash shortages. 5. Duplicitous and forgery. 6. Anomalies in foreign exchange communications. 7. Any other type of fraud not coming under the specific heads as above (Reserve Bank of India). The Reserve Bank of India is the apex body in the Indian banking system, and all the legal and regulatory requirements are governed by the RBI. (Sarla and Basvaraj, 2018).

Banks categorise the frauds mainly into three different categories, i.e. technology-related frauds, Know your customer (KYC) related frauds (deposit accounts), and advance-related frauds. Various electronic modes of payments, such as National Electronic Fund Transfer (NEFT) and Real-Time Gross Settlement (RTGS), have gained popularity in banking world transactions due to real-time impact at a lower cost. To prevent transactional fraud in these sections Reserve Bank of India (RBI) has advised banks to take preventive measures such as putting a cap on the value/numbers of beneficiaries, issuing alert systems, introducing digital signatures on bulk transactions, capturing internet protocol addresses, etc. (Chakraborty, 2013). Between 1990-1999, major bank frauds were fake currency, cheque forgery, and loan diligence, but now the scenario has shifted towards cybercrime, fraud accounts, and KYC violations (Swain and Pani, 2016)

The major type of online fraud prevailing in the Indian Banking system is *hacking,* unwillingly accessing a system to degrade or mislead the information. *Phishing*- to access private data such as passwords and usernames by emulating a reliable source. *Vishing*- a criminal activity via phone framework to access private and financial data for monetary reward. *Spamming*- undesirable and spontaneous messages sent to masses, so that many get trapped for monetary purposes. The other types of scams are e-mail spoofing, denial of administration, and ATM skimming (Rao, 2019).

Various banks use several techniques to mitigate these electronic bank frauds. The two main techniques are Artificial Neural Networks (ANN) and Geographical Information Systems (GIS). When these two techniques are aligned together, the system provides intelligent predictors of the emergence of fraudulent activities in the banking system (Eneji, 2019). Uttar Pradesh is the top leading state in terms of online fraud, followed by Maharashtra and Gujarat (Sawhney, 2024).

The paper proceeds as follows. Section 2 explains the review of related literature; Section 3 broadly discusses the research methodology; Section 4 entails the empirical findings and results, and finally, Section 4 discusses the detailed conclusion and discussion.

1. REVIEW OF LITERATURE

With the introduction of technology as a new banking system, difficulties such as financial obligations have evolved (Usman and Shah, 1970). Researchers have identified a number of potential criteria for E-banking platforms, including cost, time, security, accessibility, and fund transfer limits (Mahdi et al. 2019; Auta 2010). Among all conceivable issues, stakeholders are most concerned about security (Alaba et al. 2018; Yang et al. 2019). Furthermore, Jassal and Sehgal (2013) identified the sorts of security weaknesses in online payments that cause financial losses to both account holders and financial organisations. Soni and Soni (2013) investigated cyber fraud in the banking industry and discovered that foreign and private banks experience more cyber fraud than public sector banks.

Similarly, several studies have found fraud patterns, such as Chakrabarty (2013), who recognised the behavioural perspective of fraudland behaviours in online banking transactions. Kovach and Ruggiero (2011) empirically identify that a limited number of transactions are examined by a single hacker, which is typically attributed to password failure. Wei et al. (2013) investigated the various challenges in online banking fraud in Australia, such as dynamic fraud behaviour, weak forensic evidence, diverse customer behaviour patterns, and real-time detection, as some of the major challenges that should be addressed.

Moreover, some studies have classified electronic banking security attacks into distinct categories. For example, Vrincianu and Popa (2010) identified factors that contribute to security attacks, such as denial of service, unauthorised use, and repugnance; Dalton et al. (2006) employed the Attack Tree Model (ATM) to divide the attacks into three groups: device control, credential theft, and legitimate access. Furthermore, Brar et al. (2012), phishing, fishing, and clone voice banking systems are included in the local, remote, and hybrid categories of e-banking attacks. Ali et al. (2019) have proposed that hybrid assaults, which

© 2026 **Journal of International Commercial Law and Technology**; Volume: 7: Issue: 1| All Right Reserved

incorporate elements of both local and remote attacks, are the most potent. Examples of these attacks include Trojan, fake pop-up windows, and host profile attestation.

Extended to this, Sharma *et. al* (2011) in their study concluded that nearly 65% of the complainants felt that mobile banking was unfeasible when it comes to transferring certain applications. Customers also gave way to scammers to admittance their data stored on mobile devices, including their messages, galleries, and various files and folders encompassing intimate data theft that could lead to scams. Pasricha and Mehrotra (2014) investigated 2760 financial fraud cases and discovered that 65% of the overall cases were internet-related. This emphasizes the importance of continuous technology upgrades to address security issues stemming from technological uncertainties, which can lead to data misuse.

Gupta and Gupta (2015) acknowledged that financial fraud could be reduced through active and mindful action by auditors and corporate executives who are willing to avoid committing financial fraud despite pressure from investors, government securities regulators, and external market fluctuations. Ziegenfuss (1995) emphasised fraud surveys in local and state governments. The author conducted interviews with government auditors to assess degrees of financial fraud. Findings reveal that significant fraud challenges, along with administrative responses, are often inadequate. Further, the study found that misuse of funds, false invoicing, and misrepresentation are the primary contributors to financial fraud losses. Table 1 presents a comprehensive literature review on E-banking payment and e-payment fraud.

"Table 1 about here"

Authors	Research Methodology & Sampling	Main Results
Bhasin (2015)	Indian Banking Personnel (Primary Study)	The study recommended that to ensure the safety, integrity, and authenticity of transactions, banks can employ multi-point scrutiny, including cryptographic verification barriers.
Sood and Bhushan (2020)	Thematic Analysis (2000-2019)	After reviewing the corpus of literature, the author employed thematic analysis technique to pinpoint two major themes: the "regulatory and compliance" focus of the studies and the "socio psychological" aspect of the literature. The popularity of study areas shifted, according to a theme analysis, from areas like balance sheet or accounting frauds in the early 2000s to areas like identity theft and cyber frauds in the latter decade.
Tiwari, Agarwal & Singh (2022)	Linear Regression and Analysis of Variance (2009-2021)	The study found that despite rising transaction volumes, the study found a decrease in fraud cases over time. It recommended that the government adopt security measures, review the BVN system, and educate users about banking.
Syafitri *et. al* (2022)	Qualitative Study	The study found that biggest threats are social engineering and phishing attacks, often combined with the use of malicious software. User awareness campaigns are one of the most important remedial mechanisms against social engineering and phishing attacks that should be carried out by payment system institutions.
Libi and Pokharel (2023)	Regression Analysis (Nepal)	The feedback provided by banking clients has brought to light the significance of raising customer awareness, fortifying technology defences, and putting in place sensible rules and guidelines in order to prevent fraud in

© 2026 **Journal of International Commercial Law and Technology**; Volume: 7: Issue: 1| All Right Reserved

		the banking industry. It was found that this study is a useful tool for comprehending the dynamics of banking fraud as the banking sector develops and responds to new difficulties.
Singh and Mohapatra (2023)	One Way ANOVA (2021-22)	The study found that accounting practitioners acknowledge the existence of frauds and concur that forensic accounting can help identify and stop them; that withholding information breaches accounting convention as well as the principles of "disclosure" and transparency; and that strong organisational values are a contributing factor to frauds.
Sirohi and Misra (2024)	Primary Study (India, 2018)	The study found that digital fraud victimization is more widespread than investment fraud, and financial education considerably reduces the likelihood of victimization in both types of economic crimes. The study also found that males under the age of 60 who have completed at least high school and come from moderate to lower socioeconomic origins are more likely to be victims of digital financial fraud.
Verma and Chakarwarty (2024)	Herfindahl–Hirschman index and Z score to measure market share and financial stability.	The authors observe a negative relationship between cybercrimes and financial stability, which they credit to banks' increased vulnerability to risk as a result of FinTech competition.

Numerous studies on e-banking payments and e-payment fraud have been conducted worldwide, particularly in industrialised nations. For example, Bughin (2004) in Canada found that the national level internet adoption accounts for two-thirds of the variance in e-banking adoption. Trudeau (2009) investigated e-banking and e-payment fraud in Canada, the Netherlands, and the United Kingdom of America (USA). The literature has grown and shifted towards developing countries, particularly India (Kumar and Diwedi, 2021; Tiwari, Agarwal, and Singh, 2022; Trivedi et al., 2023), where the NPCI, a government official body, launched the Unified Payment System (UPI) platform. The introduction of this initiative resulted in a 100% increase in digital payment transactions between 2019 and 2023 (PIB, Feb 15, 2023). With the growth of e-banking transactions, e-payment fraud has also increased in India. As per reports, UPI alone accounts for 55% of all digital payment fraud in India (Aggarwal, 2023).

Our study focused on one of the 11 Himalayan states named Himachal Pradesh, based on the following reasons: firstly, there is a dearth of studies that investigate e-banking transactions and e-payment fraud in Himachal Pradesh. Secondly, in recent years, Himachal Pradesh reported a 77 per cent increase in financial frauds, social networking and miscellaneous complaints (Press Trust of India, 2023). Thirdly, as per the reports, Mandi, Shimla and Kangra are the top three targeted districts where these frauds are highly rated in Himachal Pradesh (Press Trust of India, 2023). By understanding these challenges, the current study not only contributes to the existing literature but also provides insightful recommendations for policymakers, government agencies, businesses and individuals to strengthen the e-banking security system in the region.

Objectives of the study:

The present research is based on the following objectives-

1. To examine the impact of demographics on the E-Banking Payment system in the state of Himachal Pradesh, India.
2. To access the relationship between the E-Banking Payment system on E-Payment Frauds in the state of Himachal Pradesh, India.
3. To offer suggestions to enhance the level of awareness in people related to E-Payment fraud during E-Banking Payments.

Hypothesis development:

© 2026 **Journal of International Commercial Law and Technology**; Volume: 7: Issue: 1| All Right Reserved

H_1: To note down the impact of demographics on the E-Banking Payment system.

a. **$H_{1.0}$:** Gender has no role to play in the E-Banking Payment system.
b. **$H_{2.0}$:** Occupational does not affect the E-Banking Payment system.
c. **$H_{3.0}$:** Educational level has nothing to do with the E-Banking Payment system.

H_2: There is a significant relationship between the E-Banking Payment system and E-Payment Frauds.

2 RESEARCH METHODOLOGY

SAMPLE SELECTION

To ensure representation of the state's demographic diversity, we selected Kangra, Mandi, and Shimla districts based on high population statistics, collectively constituting 48.41% of the state's population (Census, 2011). Also, these are the top three targeted districts where frauds are highly reported in Himachal Pradesh (Press Trust of India, 2023). We chose convenience sampling as it is a practical way to collect information from diverse individuals within the selected districts, helping us to gain valuable insights into e-payment adoption trends across different demographic groups. We used the Questionnaire tool for data collection as it is widely used for large data populations, as well as useful for capturing the true behaviour of the respondents. A total of 15 statements were included in the study, out of which 5 represent the demographics of respondents, and 10 represent the structure. After that, the Excel file was transferred to the SPSS software. Out of the 580 questionnaires collected, 223 were deemed unsuitable due to incomplete or irrelevant responses. Therefore, we discarded the inappropriate responses, and our final sample size comprised 357 questionnaires. This sample size aligns with the guidelines provided by Morse (2000), ensuring statistical accuracy and reliability in our research findings. Finally, the reliability of the questionnaire was assessed using Cronbach's alpha in a pilot study after 42 initial responses were received. The alpha score of 0.781 indicates the consistency and dependability of the data included in the questionnaire. The data was examined using Jamovi and Microsoft Excel. The data was edited, cleaned, sorted, and coded using Microsoft Excel, and advanced statistical analysis was performed using Jamovi.

3.STATISTICAL TOOL AND TECHNIQUES APPLIED:

For the analysis of results, various statistical tools and techniques were applied:

S. No.	Statistical test used	Purpose
1	Exploratory Factor Analysis (EFA)	The researcher used EFA for dimension reduction and to uncover the latent construct.
2	Confirmatory Factor Analysis (CFA)	Based on the findings of the EFA, the researcher used CFA for validation of the results of the EFA and to hypothesise whether the factor structure fits the data well or not.
3	ANOVA (Analysis of Variance)	This statistical technique is used to compare the means of three or more groups, making it more suitable for measuring the impact of two categorical variables, *"Occupation"* and *"Education Level",* on the E-banking payment system.
4	Independent Sample t-test.	We used the independent sample t-test to compare the mean of two independent groups on Gender (Categorical variable) and E-Banking Payment (Continuous variable)
5	Correlation analysis	The Karl Pearson coefficient of correlation was used to determine whether E-Banking Payment and E-Payment Frauds were correlated or not?

ESTIMATION RESULTS

DESCRIPTIVE STATISTICS

Descriptive statistics of demographic variables as shown in Table 2. A total of 357 respondents have joined the survey. A total of five demographic variables have been included in the study: *Age, Gender, Occupation, Educational qualification, and Bank.* 168 (47.3%) of the respondents were between the 20-29 years of age group, and only 29 (8.2%) are above 60. 247 (69.1%) out of 357 respondents are male, and 110 (30.8%) are female. 149 (41.8%) are postgraduates, and only 23 (6.4%) are M.Phil and PhD 237 (66.4%) out of a total of 357 respondents were neither in the government sector nor private business, and 39 (10.9%) were in the private sector. Out of the total 357 respondents, 166 (46.4%) have their account in the State Bank of India, 117 (32.7%) have their bank account in Punjab National Bank, and only 6 (1.8%) have their account in Grameen Bank. Further, the QQ plot and the Box plot both show that the data is normally distributed. In addition to it, two analytical tools, skewness and kurtosis, were used; the values of both of them are within threshold limits (-0.741 and 1.80), which shows that the data is normally distributed.

"Table 2 about here"

© 2026 **Journal of International Commercial Law and Technology**; Volume: 7: Issue: 1| All Right Reserved

	Levels	Counts	% of Total
Age	20-29 (level 1)	168	47.05 %
	30-39 (level 2)	95	26.6 %
	40-49 (level 3)	36	10.0 %
	50-59 (level 4)	29	8.1 %
	60 and above (level 5)	29	8.1 %
Gender	**Levels**	**Counts**	**% of Total**
	Male (level 1)	247	69.18 %
	Female (level 2)	110	30.81 %
Education level	**Levels**	**Counts**	**% of Total**
	Higher Secoundary (level 1)	75	21 %
	Graduate (level 2)	110	30.8 %
	PG (level 3)	149	41.7 %
	M.phil and Ph.d (level 4)	23	6.4 %
Occupation	**Levels**	**Counts**	**% of Total**
	Govt. Employee (level 1)	81	22.7 %
	Private Business (level 2)	39	10.9 %
	Others (level 3)	237	66.4 %
Banks	**Levels**	**Counts**	**% of Total**
	SBI (level 1)	166	46.4 %
	PNB (level 2)	117	32.7 %
	Himachal Gramin Bank (level 3)	6	1.7 %
	Others (level 4)	68	19.1 %
Normality	Skewness	-0.741	
	Kurtosis	1.81	

EXPLORATORY FACTOR ANALYSIS (EFA) SCALE VALIDATION:

Bartlett's Test of Sphericity is the technique used for redundancy analysis and guides whether the data needs reduction analysis or not based on the p-value. Here, the p-value is lower than the chosen significance (0.05), which confirms that the data needs reduction analysis. The scale validation was done through Jamovi Software, and Principal Component Factor analysis has been used with oblimin rotation. The assumption has been checked along with KMO (Kaiser- Meyer- Olkin test), and the value achieved was 0.713, which is good enough to proceed further. Factor loadings were also depicted in Tables 3 & 4 along with the scree plot. The 'minimum residual' extraction method was used in combination with an 'oblimin' rotation.

"Table 3, 4 & 5 about here"

Table 3: Bartlett's Test of Sphericity

χ^2	Df	P-Value
245	355	< .001

Table 4: Factor Loadings

	Factor		
	1	**2**	**Uniqueness**
onl-easy	0.625		0.618
onl-cash	0.622		0.558
bussi-int	0.608		0.614
atm-dc-ar	0.603		0.634
govt-ac	0.588		0.655
trust-bnk	0.416		0.827
laws-not		0.664	0.556
frd-inc		0.632	0.476
diff-pr-fr		0.593	0.653
hack-info		0.477	0.704

Table 5: KMO Measure of Sampling Adequacy

	MSA
Overall	0.713
trust-bnk	0.699
onl-cash	0.790
hack-info	0.675
atm-dc-ar	0.766
diff-pr-fr	0.564
laws-not	0.564
bussi-int	0.759
govt-ac	0.806
onl-easy	0.755
frd-inc	0.694

Source: Output from Jamovi software

FACTOR 1: E- E-PAYMENTS

There are total of 6 items that are contributing to the factor E-Payment. The 6 items are: *"In the era of modernization people fully trust banks for securing their money", "People in this world are more attracted towards online payments methods instead of cash payments", and "People have now started using A.T.M, debit cards, credit cards", "Nowadays, the Business sector is relying on the Internet for most of the business*

© 2026 Journal of International Commercial Law and Technology; Volume: 7: Issue: 1| All Right Reserved

transactions and functions in India", "Governments are encouraging people to use online payments for transactions", "Online payment mode is easy and reliable to handle". The mean of this variable is 3.90, with a minimum value of 2.00 and a maximum of 4.83, and the standard deviation is 0.559.

FACTOR 2: E-BANKING FRAUDS

The second variable comes out from EFA is E-banking Frauds that postulates total of four items, i.e. *"At the time of online payment through account number and credit card on web pages, any hacker can steal our personal information", "It is very difficult to prove monetary frauds committed on the Internet", "Indian laws are still not able to handle the financial problems in the cyberspace", "Cyber Frauds are increasing day by day in the context of monetary frauds during online shopping.* The mean value of the variable is 3.67, along with the standard deviation of 0.670. The minimum value is 1.75, and the maximum value is 5.00.

RELIABILITY:

After exploring the two factors, the reliability of the scale is checked through two statistical tools that are Cronbach's alpha and which value is 0.745, and McDonald's omega, is 0.751. The reliability of the two constructs is also checked, and the values are within the threshold limits.

CONFIRMATORY FACTORY ANALYSIS:

The two constructs that were extracted through exploratory factor analysis are now confirmed with confirmatory factor analysis. The results of the same are reported in Table 6 confirms the robust relationship between indicators and their respective factors. Notably, indicators such as "onl-cash" and "frd-inc" possess strong loading onto their respective factors. Further, χ^2 test value is 47.5, and the p-value is 0.29, which suggests that there is no significant lack of fit between the model and observed data (Table 7). Along with that, other fit measures such as Comparative Fit Indices (CFI), Tucker Lewis Indices (TLI), Root Mean Square Error of Approximation (RMSEA) and Standardised Root Mean Square Residual (SRMR) indicated acceptable model fit, providing confidence in the adequacy of the measurement model (reported in Table 7).

"Table 6 & 7 around here"

Factor	Indicator	Estimate	SE	Z	p	Std. Estimate
E-Payment	trust-bnk	0.315	0.0872	3.61	< .001	0.381
	onl-cash	0.595	0.0904	6.58	< .001	0.651
	atm-dc-ar	0.420	0.0684	6.15	< .001	0.610
	bussi-int	0.519	0.0815	6.37	< .001	0.634
	govt-ac	0.496	0.0846	5.86	< .001	0.589
E-Frauds	onl-easy	0.531	0.0921	5.77	< .001	0.578
	hack-info	0.541	0.1162	4.66	< .001	0.564
	diff-pr-fr	0.396	0.1102	3.59	< .001	0.393
	laws-not	0.292	0.0947	3.08	0.002	0.319
	frd-inc	0.760	0.1195	6.36	< .001	0.893

Source: Output from Jamovi Software

Test for Exact Fit		
χ^2	**Df**	**P-Value**
47.5	355	0.029

Fit Measures

Particulars				**RMSEA 90% CI**	
CFI	**TLI**	**SRMR**	**RMSEA**	**Lower**	**Upper**
0.932	0.907	0.0702	0.0632	0.00403	0.101

Residual Covariances – Modification Indices

	trust-bnk	onl-cash	atm-dc-ar	bussi-int	govt-ac	onl-easy	hack-info	diff-pr-fr	laws-not	frd-inc
trust-bnk	1	0.977	1.83	0.578	0.439	0.043	0.189	1.666	2.383	4.399
onl-cash		1	0.230	0.639	2.22	1.567	2.749	0.047	0.803	0.009
atm-dc-ar			1	0.174	0.094	0.064	3.331	3.143	2.681	1.263

© 2026 Journal of International Commercial Law and Technology; Volume: 7: Issue: 1| All Right Reserved

bussi-int				1	3.847	1.029	0.109	5.601	1.149	3.931
govt-ac					1	0.2277	0.9034	0.276	0.072	0.282
onl-easy						1	0.0813	1.179	5.081	1.340
hack-info							1	0.410	0.002	2.643
diff-pr-fr								1	0.964	0.524
laws-not									1	1.412
frd-inc										1

Source: Output from Jamovi software

INDEPENDENT SAMPLE T-TEST, ANOVA AND KARL PEARSON COEFFICIENT OF CORRELATION:

GENDER DOES NOT AFFECT THE E-PAYMENT SYSTEM.

Table 8 depicts the results of the independent sample t-test on three demographic profiles of the online payment system. Table 8 indicates the assumptions checked by the homogeneity test of variance (Levene's Test). An independent-sample t-test was conducted to compare the role of gender (Male and Female) in the E-payment system. Since the p-value is greater than the significance level of 0.05, we fail to reject the null hypothesis that Gender does not affect the E-payment system. Our findings are consistent with previous research; for example, Shree et al. (2021) found no discernible gender differences in the electronic payment process.

"Table 8 around here"

Particulars							**95% Confidence Interval**	
		Statistic	**df**	**P**	**Mean difference**	**SE difference**	**Lower**	**Upper**
E-Banking Payment	Student's t	-0.577	355	0.565	-0.0667	0.116	-0.296	0.162

Homogeneity of Variances Tests					
Particulars		**F**	**df**	**df2**	**P**
E-Banking Payment	Levene's	1.14	1	355	0.288
	Variance ratio	0.545	246	109	0.031

Source: Output from Jamovi software

OCCUPATIONAL DOES NOT AFFECT THE E-BANKING PAYMENT.

Table 9 reports the result of the ANOVA test signifies the profile of two demographic constructs that are occupation and educational level, on the E-Banking Payment system. ANOVA performs two means- the sum of squares and mean squares, respectively. In the first table, based on the p-value, the evidence clearly favours the acceptance of the null hypothesis, as the p-value is greater than 0.718, surpassing the significance level. This suggests that occupation does not significantly affect the e-payment system in Himachal Pradesh. Our findings are consistent with the study by Shree et al. (2021), which observed that unemployed individuals and homemakers utilized online payment systems less frequently than salaried employees.

"Table 9 around here"

© 2026 **Journal of International Commercial Law and Technology**; Volume: 7: Issue: 1| All Right Reserved

Particulars	Sum of Squares	df	Mean Square	F-Stat	P-Value
Overall model	0.210	2	0.105	0.333	0.718
occup	0.210	2	0.105	0.333	0.718
Residuals	33.801	355	0.316	0.616	0.824
Homogeneity of variances tests					
Particulars	**Statistic**	**df**	**Df2**	**P-Value**	
Levene's	0.336	2	355	0.716	
Bartlett's	0.840	2	355	0.657	

Source: Output from Jamovi Software

EDUCATIONAL LEVEL HAS NOTHING TO DO WITH THE E-BANKING PAYMENT.

Table 10 reports the results of an ANOVA test, indicating the influence of educational qualifications on the E-payment system in the provided data. The p-value of 0.636 exceeds the significance level of 0.05, indicating no significant evidence to reject the null hypothesis. The study's findings were not statistically significant, indicating that education level does not play a significant role in using the e-payment system. This contrasts with the findings of Shree et al. (2021), which suggested an enabling effect of education on e-payment system usage. Furthermore, Jiménez and Díaz (2019) demonstrated in their study that individuals with higher educational levels and incomes are less likely to use Internet banking, potentially due to a preference for personalised advice when making decisions about investments in more complex financial products.

"Table 10 around here"

Particulars	Sum of Squares	df	Mean Square	F-Stat	P-Value
Overall model	0.540	3	0.180	0.570	0.636
edu	0.540	3	0.180	0.570	0.636
Residuals	33.471	353	0.316		
Homogeneity of Variances Tests					
Particulars	**Statistic**	**df**	**df2**	**P-Value**	
Levene's	1.06	3	353	0.369	
Bartlett's	4.51	3	353	0.211	

Source: Output from Jamovi Software

E-BANKING PAYMENT DOES NOT RELATE WITH E E-PAYMENT FRAUDS.

The correlation results indicate a statistically significant, but low positive correlation ($r = 0.161$, $p < 0.05$) between E-banking payment and E-payment fraud in Himachal Pradesh. The state's high literacy rate is further supported by the low correlation, which suggests that a sizable section of the population is educated and may be more knowledgeable about digital security procedures. Furthermore, digital literacy initiatives and awareness programs launched by the Himachal Pradesh government enable citizens to make informed decisions when making online transactions. Understanding the risks connected with E-payments and having the ability to recognise potential threats minimises the likelihood of becoming a victim of E-fraud.

"Table 11 around here"

Variables	Pearson's r	p-value
E - Payment	-	-
E - Fraud	0.161	*<0.05*

Source: Output from Jamovi software

DISCUSSION & CONCLUSION

It is found in the research that the respondents belonging to the state of Himachal Pradesh are somewhat aware of E-banking services and E-frauds associated with these services. State Bank of India is the leading branch among bank, and most of the respondents have their accounts in SBI. Punjab National Bank is the second preferred choice, as there are a lot of army pensioners in the district. Respondents rely mostly on other banks, and the least preferred choice is Himachal Pradesh State Cooperative Bank. With the 86.6% literacy rate of Himachal Pradesh (92.9% Male and 80.5% Female) (NFHS-5, 2021), people are aware of all the things happening around, and technology has given them this path to achieve. The survey depicts that there is no role of gender to play when it comes to performing E-payments. The respondents of the research are from Mandi, having a literacy rate of 91.56% then Kangra district literacy rate of 85.67% and Shimla district with 93.63% literacy rate. Most of the respondents are postgraduates and are aware of all the banking systems in detail, along with the fraud associated with the banking system. the survey rejects the role of education in making E-payments. The primary reason for that is the literacy rate, and the second is technological advancement. Technological advancements made youth aware of all the possible consequences, as most of the respondents are between the ages group 20-30. Kangra, Shimla and Mandi are the three most populous districts of Himachal Pradesh as per the Census-2011 and Adhaar data 2021-22. Various growing business opportunities by state and central governments in the state also make them aware of instant transactions. Occupation also has nothing to do with E-payments. E-payments have a significant effect on E-frauds but negligibly. The main reason for this is that banks are now constantly updating the security in the E-payments. Literacy rate and various awareness programs, and 3D banking security systems initiated by banks.

Reserve Bank of India launched various programs against phishing links, vishing calls, ATM card skimming, juice jacking, and others. Be(A)WARE is the booklet launched by RBI that mentions all the scams and

© 2026 Journal of International Commercial Law and Technology; Volume: 7: Issue: 1| All Right Reserved

frauds along with prevention and precautionary systems, but still, there is a slight increase in internet banking frauds. Department of Financial Services under the Ministry of Finance launched and linked various schemes to aware people related to e-frauds. SBI has also launched against KYC fraud on various social media platforms and also issued a helpline *cybercrime.gov.in* for all reports against KYC fraud. Banks also initiated regular communication with their customers through calls and messages to never share OTP, CVV, or ATM pins with anyone, including bank officials. This is the reason why people are now becoming conscious of e-frauds.

Like every study, the study faces some limitations that must be considered when interpreting the findings. Firstly, the selection of Kangra, Mandi, and Shimla districts, while based on their high population statistics, may introduce bias as other districts with different socio-economic characteristics were not included. Secondly, the use of convenience sampling may result in a non-representative sample, as respondents were chosen based on their easy accessibility rather than through random selection. This could lead to an overrepresentation or underrepresentation of certain demographic groups, affecting the reliability of our conclusions. Additionally, discrepancies in response rates between online and offline distribution methods could also skew the results, particularly if certain demographic groups are more inclined to respond through one mode over the other. Finally, the study's focus primarily on e-payment adoption trends within urban and rural settings of the selected districts may overlook other influential factors such as technological infrastructure, government policies, and cultural attitudes towards e-payments. Recognising these limitations is crucial for interpreting the study's results accurately and ensuring the validity of our research findings[2].

References:

1. Aggarwal, R. (2023, May 16). UPI-related scams account for 55% of total digital payments frauds in India. www.business-standard.com. https://www.business-standard.com/finance/news/upi-related-scams-account-for-55-of-total-digital-payments-frauds-in-india-123051600333_1.html
2. Alaba, F. A., Hakak, S., Khan, F. A., Adewale, S. H., Rahmawati, S., Patma, T. S., ... & Herawan, T. (2018). Model-Based Testing for Network Security Protocol for E-Banking Application. In Information Systems Design and Intelligent Applications: Proceedings of Fourth International Conference INDIA 2017 (pp. 740-751). Springer Singapore.
3. Ali, M. A., Hussin, N., & Abed, I. A. (2019). E-banking fraud detection: a short review. Int. J. Innov. Creat. Chang, 6(8), 67-87.
4. Article, R. (2020). Significance of fraud analytics in Indian banking sectors. 7(4), 209–213.
5. Auta, E. (2010). E-banking in developing economy: Empirical evidence from Nigeria. Journal of Applied Quantitative Methods, 5(2): 212 – 222.
6. Bhasin, Madan Lal, Menace of Frauds in the Indian Banking Industry: An Empirical Study (October 20, 2015). Australian Journal of Business and Management Research, Vol. 4 No. 12, April-2015, Available at SSRN: https://ssrn.com/abstract=2676466 http://dx.doi.org/10.2139/ssrn.2676466
7. Bhatia, P. A., Sivakumar, S. N. V, & Agarwal, A. (2016). A Contemporary study of microfinance : A study for India ' s underprivileged. 23–31.
8. Brar, T. P. S., Sharma, D. & Khurmi, S. S. (2012). Vulnerabilities in e-banking: A study of various security aspects in e-banking. International Journal of Computing & Business Research, 6: 127-132.
9. C., Bhavan, C. O., & Marg, S. S. (2017). Department of Banking Regulation,Central Office, 12th & 13th Floor, Central Office Bhavan, ShahidBhagat Singh Marg, Mumbai - 400001.
10. Chadha, N. (2017). An Analytical Study of Reforms and their Impact on Indian Banking Sector. International Journal of Business Administration and Management, 7(1), 2278–3660. http://www.ripublication.com
11. Chakrabarty, K. C. (2013). Fraud in the banking sector—causes, concerns and cures. In National Conference on Financial Fraud organised by ASSOCHAM, New Delhi, 26.
12. Chakrabarty, K.C. (2013). Fraud in the banking sector – causes , concerns and cures. Central, B. I. S. July, 1–13.
13. Dalton, Mills, Colombi, & Raines. (2006, June). Analyzing attack trees using generalized stochastic petri nets. In 2006 IEEE Information Assurance Workshop (pp. 116-123). IEEE.
14. Dubey, R. D., & Manna, A. (n.d.). E-Banking Frauds And Fraud Risk ManagemenT. 1632, 20–23.
15. Fernandes, L. (2013). Fraud in electronic payment transactions: threats and countermeasures. 2(3), 23–32.
16. Global Banking Fraud Survey. (2019). Global Banking Fraud Survey 2019 -The multi-faceted threat of fraud: Are banks up to the challenge? May, 1–24. https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/05/global-banking-fraud-survey.pdf
17. Granville, A., Jorge, A., Barreto, B. E., & Silva, R. D. (2019). Impact of Frauds on the Indian Banking Sector. 7, 219–223.
18. Gupta, P. K and Gupta, S. (2015) Corporate Frauds in India- Perceptions and Emerging Issues, Journal of Financial Crime, Vol. 22 (1), pp. 79-103

[2] *Id.*

© 2026 **Journal of International Commercial Law and Technology**; Volume: 7: Issue: 1| All Right Reserved

19. Helmi, H., & Hadidi, E. (2018). Impact of Microfinance on Entrepreneurial Development : The Case of Egypt. 9(9), 68–76. https://doi.org/10.30845/ijbss.v9n9p
20. Jassal, R. K., & Sehgal, R. K. (2013). Online banking security flaws: a study. International Journal of Advanced Research in Computer Science and Software Engineering, 3(8), 1016-1021.
21. Jhamb, A., & Jhamb, S. (2017). Microfinance and Entrepreneurship Development. VI(Ii), 54–56.
22. Journal, I., Vol, S. S., Factor, I., & Homepage, J. (2020). A Descriptive Study on Frauds in Various Banking Operations of India Dr. Gulshan Kumar Associate Professor, Rajshree Institute of Management & Technology, Bareilly. 10(03), 104–113.
23. Khan, I. (2014). Performance of regional rural banks : a case study. 3(1), 2010–2011.
24. Kovach, S., & Ruggiero, W. V. (2011, February). Online banking fraud detection based on local and global behavior. In Proc. of the Fifth International Conference on Digital Society, Guadeloupe, France (pp. 166-171).
25. Kumar, M., Bohra, N. S., & Johari, A. (2010). Micro-Finance as an Anti Poverty Vaccine for Rural India. 2(1), 29–35.
26. Kumar, N., & Diwedi, D. N. (2021). Digital fraud and advancement of fraud mitigation mechanisms in India. VIDHIGYA: The Journal of Legal Awareness, 16(1and2), 18-22.
27. Lal, T. (2014). Measuring impact of financial inclusion on rural development through cooperatives. https://doi.org/10.1108/IJSE-02-2018-0057
28. Libi, Er. Sujit Kumar and Pokharel, Post Raj, A Survey on Banking Fraud in Chitwan, Nepal: Banking Customers' Perspective (November 5, 2023). Available at SSRN: https://ssrn.com/abstract=4623878 or http://dx.doi.org/10.2139/ssrn.4623878
29. Mahdi, M. H., Abdulrazzaq, A. A., Rahim, M. S. M., Taha, M. S., Khalid, H. N., & Lafta, S. A. (2019, May). Improvement of image steganography scheme based on LSB value with two control random parameters and multi-level encryption. In IOP Conference Series: Materials Science and Engineering (Vol. 518, No. 5, p. 052002). IOP Publishing.
30. Misal, D. M. (2013). A study of role of micro-finance in rural empowerment in india. 3(1), 37–41.
31. Morse, J. M. (2000). Determining sample size. Qualitative health research, 10(1), 3-5.
32. Mohanty, S. (n.d.). On the Recent Scams and Frauds in Indian Banking System.
33. Ms, P., Sayed, G., & Trivedi, P. (n.d.). Role of Micro Finance Institutions in Development of Micro- Enterprises (MSMEs) in Mumbai - An Empirical Study. 51–61.
34. Newman, A., & Schwarz, S. (2017). i s b j Microfinance and entrepreneurship : An introduction. November. https://doi.org/10.1177/0266242617719314
35. Ogbe, A. A. (2017). Microfinance & Entrepreneurship Development. December 2015.
36. Patil, R., & Kamath, V. (2017). " Impact of Microfinance on Rural development " (With special Reference to Gulbarga Division of Karnataka State). 19(9), 1–9. https://doi.org/10.9790/487X-1909010109
37. Payment Threats and Fraud Trends Report. (2019). European Payments Council, December. https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2019-12/EPC302-19 v1.0 2019 Payments Threats and Fraud Trends Report.pdf
38. Press Trust of India. (2023, December 3). In Himachal, one cyber crime complaint per hour. Hindustan Times. https://www.hindustantimes.com/cities/chandigarh-news/in-himachal-one-cyber-crime-complaint-per-hour-101701546992334.html
39. Rana, S. (2017). Role of micro financing in development of rural areas of Shimla , Himachal Pradesh , India. 693–695.
40. RBI. (2013). Banking Structure in India - The Way Forward Reserve Bank of India. August, 1–88. https://rbi.org.in/Scripts/PublicationReportDetails.aspx?ID=713#2
41. Report, A. A. (2018). Okkf " kZd iz ' kklfud izfrosnu Department Of Rural Development. 18.
42. Roy, A. (2007). Microfinance and Rural Development in the North East India. 43–56.
43. Sawhney, A. (2024, February 6). Around 1.1 million financial fraud cases registered in 2023, shows data. www.business-standard.com. https://www.business-standard.com/india-news/around-1-1-million-financial-fraud-cases-registered-in-2023-shows-data-124020601528_1.html
44. Science, C., & Studies, M. (2013). Rural Entrepreneurship in India : Challenge and Problems. 1(2), 28–37.
45. Shah, M. (2019). A Case Study on Increasing of Banking Frauds in India. 2(1), 20–23.
46. Singh Rao, H. (2019). Cyber Crime in Banking Sector. International Journal of Research - GRANTHAALAYAH, 7(1), 148–161. https://doi.org/10.29121/granthaalayah.v7.i1.2019.1043
47. Singh, C., & Antony, K. (2016). Frauds in the Indian Banking Industry. March, 1–24.
48. Singh, N. P. (2007). Online Frauds in Banks with Phishing. Journal of Internet Banking and Commerce, 12(2), 1–28. http://eprints.utm.my/8136/
49. Singh, R and Das, A.K. Mohapatra. (2023). Awareness, Causes and Measures for prevention of Corporate Frauds in India-An Empirical Study. European Economic Letters (EEL), 13(4), 875–903. https://doi.org/10.52783/eel.v13i4.673

© 2026 **Journal of International Commercial Law and Technology**; Volume: 7: Issue: 1| All Right Reserved

50. Sirohi, N., Misra, G. Vulnerability of individuals to economic crime and the role of financial literacy in its prevention: Evidence from India. Crime Law Soc Change (2024). https://doi.org/10.1007/s10611-024-10138-w
51. Soni, R.R and Soni, N. (2013), "An Investigative Study of Banking Cyber Frauds with Special Reference to Private and Public Sector Banks", Research Journal of Management, Sciences, Vol. 2(7), pp. 2227.
52. Sood, P., Bhushan, P. A structured review and theme analysis of financial frauds in the banking industry. Asian J Bus Ethics 9, 305–321 (2020). https://doi.org/10.1007/s13520-020-00111-w
53. Swain, S., & Pani, L. K. (2016). Frauds in Indian Banking : Aspects , Reasons , Trend-Analysis and Suggestive Measures. 5(7), 1–9.
54. Swapna, K. (2017). Impact of Microfinance on Women Entrepreneurship. 7(1), 229–241.
55. Syafitri, W., Shukur, Z., Asma'Mokhtar, U., Sulaiman, R., & Ibrahim, M. A. (2022). Social engineering attacks prevention: A systematic literature review. IEEE access, 10, 39325-39343.
56. Thakur, S. (2019). Electronic Banking Fraud in India : Effects and Controls. 8(10), 823–829.
57. Tiwari, S., Agarwal, P., & Singh, R. (2022). Assessment of Association between Financial Fraud Cases in reference to Transaction Volume & E-Auditing. Pacific Business Review International, 14(11), 37-44.Sarala, M. S. (2018). E-Banking Frauds and RBI Guidelines. 409–416.
58. Tiwari, S., Agarwal, P., & Singh, R. (2022). Assessment of Association between Financial Fraud Cases in reference to Transaction Volume & E-Auditing. Pacific Business Review International, 14(11), 37-44.
59. Total digital payment transactions volume increased from 2,071 crore in FY2017-18 to 13,462 crore in FY2022-23 at a CAGR of 45%. (2023, December). Reserve Bank of India (RBI), National Payments Corporation of India (NPCI). https://pib.gov.in/PressReleasePage.aspx?PRID=1985240
60. Trivedi, S. K., Vishnu, S., Singh, A., & Yadav, M. (2023). Research trends in sustainable E-payment systems: A study using topic modeling approach. IEEE Transactions on Engineering Management.
61. UK Finance. (2019). Fraud The Facts 2019 , The definitive overview of payment industry fraud. 1–53. https://www.ukfinance.org.uk/system/files/Fraud The Facts 2019 - FINAL ONLINE.pdf
62. Usman, A. K. & Shah, M. H. (1970). Critical success factors for preventing e-banking fraud. The Journal of Internet Banking and Commerce, 18(2): 1-14.
63. Vaidya, M. (2018). Factors Affecting Financial Inclusion in Himachal Pradesh : A District-wise Analysis. 3(1), 54–65.
64. Verma, D. and Chakarwarty, Y. (2024), "Impact of bank competition on financial stability-a study on Indian banks", Competitiveness Review, Vol. 34 No. 2, pp. 277-304. https://doi.org/10.1108/CR-07-2022-0102
65. Vrancianu, M. & Popa, L. A. (2010). Considerations regarding the security and protection of e-banking services consumers' interests. The Amfiteatru Economic Journal, 12(28): 388-403.
66. Wei, W., Li, J., Cao, L., Ou, Y., & Chen, J. (2013). Effective detection of sophisticated online banking fraud on extremely imbalanced data. World Wide Web, 16, 449-475.
67. Yang, L., Elisa, N., & Eliot, N. (2019). Privacy and security aspects of E-government in smart cities. In Smart cities cybersecurity and privacy (pp. 89-102). Elsevier.
68. Zeigenfuss, D.E. (1996), "State and Local Government Fraud Survey for 1995". Managerial Auditing Journal, Vol. 9, pp. 49.

© 2026 **Journal of International Commercial Law and Technology**; Volume: 7: Issue: 1| All Right Reserved