Empowering Consumers: The Importance Of Security Awareness In India's Digital Payment Ecosystem

Ubaid Shaik
School Of Management Studies
Chaitanya Bharathi Institute Of Technology
Hyderabad,India

Dr Sowmya Kethi Reddi
School Of Management Studies
Chaitanya Bharathi Institute Of Technology
Hyderabad,India

Dr T.S.Poorna Chandrika
School Of Management Studies
Chaitanya Bharathi Institute Of Technology
Hyderabad,India

***Abstract*—Over the last few years, the country has been witnessing a drastic change in the integrated and innovative financial structures to some extent facilitated through digital payments systems. And such change has benefited the consumer as they are able to complete transactions effortlessly through easy accessible and efficient means. However, since the use of digital payments is increasing, it also came with several security problems that a customer will encounter. In this research paper, one of the components of consumers' security knowledge, security consciousness in the context of the mobile payment system in India. In the current work, using the specifics of the structured questionnaire, the assessment of consumers' knowledge, attitudinal beliefs, and behavioral changes relating to digital payment security is conducted. These outcomes show the rather low level of securities consciousness among the users, thus the undertaking of special educational and information activities, as well as high security demands in the PSPs. If all the related stakeholders insist on people being more security minded, then they will be contributing positively towards making consumers have faith in the utilization of electronic payments hence promoting sustainable electronic payment in India. Finally, this paper posits that more attention should be accorded to this factor of involving the consumers in the improvement of security and consumer protection of the digital payment systems.**

Keywords—Digital Payment Security, Consumer Trust, Security Awareness, Fraud Prevention, User Behavior, Educational Campaigns, Biometric Authentication

I. INTRODUCTION

Over the last few years, India has observed the shift within its financial industry exponentially especially centred on the usage of digital money transfer apps. The topic "Empowering Consumers: Based on this new dynamics of the digital payment environment, the paper "The Importance of Security Awareness in India's Digital Payment Ecosystem" comes out as a topic of major concern. This paper finds that an understanding of the importance of security awareness is crucial as digital transactions gain more acceptance in the ecosystem.

There may not be a more relevant topic to address in the contemporary Indian setting than this. Given the leadership's drive toward the mobile wallet economy and the availability of smartphones and internet connections, digital payments have gained much popularity in the country. By now, the number of digital payment transfers in the country has skyrocketed, and, in particular, solutions such as UPI. Nevertheless, this increased growth has been associated with an equal increase in the risks involving cybercrimes and fraud, which makes security literacy to be an artificial need for consumers. With the increase in activities such as e-commerce activities the possible hazards linked to poor security awareness enhance.

Making consumers secure aware in digital payments means that the customers themselves can fend off different types of cyber threats. Most of these users still lack adequate awareness of possible dangers involved in making business transactions online, for instance being trapped by phishing scams, having their identity stolen, or having their financial details disclosed to other people by the Web sites they visited. Such ignorance often results to substantial losses throughout and distrust in digital payment systems. Through encouraging security awareness amongst the consumers, preparation adequate to enable them to distinguish dangers and eradicate them is provided which leads to an increased confidence for using the various digital payment platforms.

In addition, security awareness is not only a consumer problem but also a financial institution, payment service providers, and regulatory agencies' concern. Such stakeholders need to put efforts together to ensure the future consumer education and security standards. It is for this reason that other measures such as workshops, online materials, as well as security features easy to understand and implement have shown to greatly improve consumer awareness. This way, stakeholders play an important role in ensuring that best practices for digital security are achieved this improves the competitive environment of the users within the DPSS model.

The research question guiding this study is: The research question for this study is as follows; To what extent does security awareness affect consumer behaviour and perceived credibility of India's digital payment system?. This research proposal focuses on the following question: To what extend does the level of perceived security influence the consumers' behaviour in terms of using services offered by digital markets? Studying this phenomenon, the research aims to define best practices to increase security consciousness and to improve security conditions of digital payment system.

II. REVIEW OF LITERATURE

In recent years, the evolution of digital payment systems in India has been so fast that transactions are becoming

more convenient and easier to make. While this shift has come with some challenges, the most prominent concern has been security, and educating the consumer. This literature review summarises existing research regarding digital payment systems, security awareness and consumer behaviour and identifies gaps, which the current study attempts to fill.

A. Digital Payment Systems

With the Indian government's thrust into making India a cashless economy, it has become an attractive option to other digital payment systems. According to research, different modes of digital payments, like Unified Payments Interface (UPI), mobile wallets, and net banking have now become part and parcel of everyday transactions (Singhal, 2021). These systems are convenient and efficient, as studies outline (Sujith and J. C., 2017). Nevertheless, the literature also indicates the risks to these systems – including cyber fraud and data breaches – that can harm consumer trust (Fernandes, 2013; Neha Priya & J. A., 2021).

Research has centred on the role of digital payment systems as influencing factors of consumer behaviour. For example, Gupta and R.K (2020) noticed that if the ease of use and benefits perceived to digital payments were high, then consumers were very willing to use these technologies. The literature, however, points out that despite the growing prevalence of payment by digital means, consumers are often reluctant to adopt the latter in some places including in rural areas (Ruangmei & Gethe, 2023). It emphasizes the necessity of targeted educational activities that would, in turn, increase consumer confidence in doing digital transactions.

B. Security Awareness

Use Security awareness is key to successful fruition of digital payment systems. Overall, research also finds that consumers who know all there is to know about the phishing scams and identity theft are more prone to doing so when they're conducting their business online. The study of Priya and J. A. (2021) reveals that most users unaware of the digital payment system security features which pose users at higher risk of cyber threats. In fact, there has long been the fact that the prevalence of such lack of awareness is particularly concerning given the growth of cybercrime among digital payments, as shown by research, e.g.((Deng & N.R., 2019; Chang & L.M., 2022)).

In addition, it is evident from the literature that security awareness is not a private issue but a social issue in relation to both the financial institutions and the payment service providers as well as the regulatory bodies. Critical communication strategies and educational programs are needed to empower consumers in the knowledge required to protect themselves in this digital payment landscape by Rama Vedashree and Nath Parameshwaran (2020). However, there is no relevant research about the impact of such educational initiatives on consumer behaviour.

C. Consumer Behavior

The Factors such as trust, perception and consumer's past experience with online fraud affect consumer behaviour in the context of digital payments (Shree & B. P, 2021). It has been studied that the understanding about security measures has a significant impact on consumers trust in digital payment systems as well as their previous experiences with fraud (Vinitha & D., 2020). The security awareness in making consumer decide to go for digital payment is important.

Despite this considerable amount of research on the consumer behaviour side, there is a comprehensive research work available that focus on the interplay between consumer security awareness and their trust in India's digital payment ecosystem. However, most other studies focus on consumer behaviour or security awareness in isolation, and have not examined how these two dimensions relate and influence overall consumer engagement with digital payment systems.

D. Gaps in the Literature

While existing research offers useful thoughts on digital payment systems, security awareness and consumer behaviour, there is still some gaps. Finally, more empirical studies of the direct relationship between security awareness and trust in digital payment systems are needed. It is important to understand this relationship when trying to craft effective strategies to improve consumer confidence and reduce risk and exposure to digital transactions.

Secondly, there is no comprehensive literature on the effectiveness of such security awareness programs in India. Some studies emphasize education's importance compared to little empirical evidence to the effect of particular initiatives on how consumers behave and screen their security practices.

Lastly, there is a call for research into security awareness and digital payment adoption, taking into account the multiple demographic factors that drive security awareness and digital payment adoption. Studies have suggested that, for example, urban consumers know more about digital payment systems than rural consumers (Ruangmei & Gethe, 2023). Yet there is still work to be done in refining the understanding of these factors: age, education, and socio economic status on security awareness and consumer behaviour in the context of digital payment.

Finally, this literature review highlights the principle of security awareness that deepens consumers' engagement within India's digital payment ecosystem. The present study attempts to make a small contribution to the understanding of how security awareness impacts consumer behaviour and trust, leading to a safer and productive digital payment landscape in India, by filling the existing gaps.

III. Research Methodology

This study explores the effect of the security awareness on users' behaviour and trust in the digital transaction system, particularly since ownership of digital payment facility in India has been demonetized. In achieving this, a quantitative research design underpinned by a structured questionnaire distributed via Google Forms was used. To gather data on several aspects of digital payment systems (consumer perceptions, experience with online fraud, and the salient factors of payment behaviour), the questionnaire was designed. Surveyed was a diverse population across various localities in India, which included urban and rural consumers. Participants were selected using a simple

random sampling technique and were thus 100+ respondents consisting of working professionals, students, and from all socio economic backgrounds.

Data collected were primary and secondary. The structured questionnaire was designed to gather primary data and the existing literature, research paper and reports on digital payments and security awareness were used to gather secondary data. For analysis of the collected data, various statistical tools like descriptive statistics to summarize the demographic information, as well as frequency analysis to find the trends in the consumer behaviour were carried. We performed correlation analysis to see the relationship between security awareness and consumer's trust on digital payment systems. Findings were presented with the use of visual aids — charts, graphs, etc. — to aid with comprehension. All around the research process, ethical considerations were given priority at the expense of participant anonymity and informed consent. The purpose of this methodology is to achieve valuable insights into what the factors are that affect the uptake of digital payment systems and the part that security awareness plays in influencing consumer behaviour in India's financial marketplace.

Objective 1: To evaluate consumer knowledge or awareness regarding digital payment systems.

Objective 2: To identify the key security threats and challenges in digital payment systems.

Objective 3: To examine consumers' attitudes towards security features.

Objective 4: To measure the impact of security awareness on consumer trust.

Objective 5: Identify effective strategies for improving security awareness.

H0 (Null Hypothesis):There is no significant difference in consumer security awareness regarding digital payment systems in India.

H1(Alternative Hypothesis):There is a significant difference in consumer security awareness regarding digital payment systems in India.

This paper adopts a structured questionnaire in assessment of consumer knowledge and attitudes towards

the digital payment security. The result makes H0 null hypothesis (H0) rejected at the significance level of less than 5% on SPSS data analysis, which means that security awareness plays a vital role in enhancing consumer trust in digital payment systems.

IV. Data Analysis And Data Intepretion

In this section, data collected through the structured questionnaire to understand consumer behaviour towards the digital payment systems in India was analysed and interpreted. SPSS is used in conjunction to perform the analysis and descriptive statistics are used to summarise the demographic characteristics of the respondents and their responses on different object on the digital payment awareness, security concerns and consumer trust.

The demographic analysis finds a diverse sample with regards to age, gender, education, occupation, income, and residential area. This helps because first it makes very interesting the point that everything cannot be data explained, because there can be diversity in how certain demographics impact the way they perceive digital payments. Take for example age and education level could be correlated with familiarity and comfort with digital payment technologies and with income level and frequency of usage.

Objectives 1 through 4 examine consumer knowledge, security concerns, attitudes regarding security features, and security awareness on trust in digital payment systems. Frequency distributions and mean scores give an idea about how much of it the consumers are aware of and also how much concerned they are about it. For instance, lack of consumer education in familiarity with the digital payment systems and perceived security risks are indicated in response to questions on the same.

In addition, the comparison between the two demographic questions (7 and Objective 4) permits us to assess the relationship between security-awareness and actual use patterns. Understanding how consumer awareness of security features shapes how consumer trusts digital payment methods requires this relationship.

age

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Below 18	14	11.4	11.4	11.4
	18 - 25	71	57.7	57.7	69.1
	26 - 35	20	16.3	16.3	85.4
	Above 55	18	14.6	14.6	100.0
	Total	123	100.0	100.0	

Fig-1

Fig-1: Analysis of its age distribution shows in large part the presence of young adults; 57.7% being aged from 18 to 25. The implication is that the survey draws the substantial portions of digital payment behaviors insight from a younger demographic, which may color the entire findings.[2]

gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	101	82.1	82.1	82.1
	Female	22	17.9	17.9	100.0
	Total	123	100.0	100.0	

Fig-2

Fig-2: Respondents distribute unequally around the Gender, with 82.1% of males (1) and 17.9% of females. The findings about digital payment behaviours and preferences may depend on this imbalance.[2]

education

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	High School	14	11.4	11.4	11.4
	Bachelor's Degree	71	57.7	57.7	69.1
	Master's Degree	30	24.4	24.4	93.5
	Doctorate	8	6.5	6.5	100.0
	Total	123	100.0	100.0	

Fig-3

Fig-3: Respondents' education levels are strongly skewed towards higher education with 57.7 percent having a Bachelor's degree and 24.4 percent completing a Master's degree.[1] This implies that views of digital payments from the survey would likely also be driven by a well educated demographic.

occupation

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Student	85	69.1	69.1	69.1
	Employed (Private Sector)	28	22.8	22.8	91.9
	Self - employed	10	8.1	8.1	100.0
	Total	123	100.0	100.0	

Fig-4

Fig-4: The occupation distribution of the respondents reveals that students with 69.1 percent predominate in the sample, followed by the employed in private sector at 22.8 percent.[1] The skew towards a student demographic may affect the insights obtained from digital payment behavior and preferences. [2]

income

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Below 25,000	78	63.4	63.4	63.4
	25,001 - 50,000	20	16.3	16.3	79.7
	50,001 - 1,00,000	17	13.8	13.8	93.5
	1,00,001 - 2,00,000	8	6.5	6.5	100.0
	Total	123	100.0	100.0	

Fig-5

Fig-5: Respondents' income distribution suggests that a large major 63.4% to be below ₹25,000 which is income of lower scale. [1] Financial constraints may influence their digital payment behaviors and preferences because these could also heavily influence their uptake of technology driven payment methods.[2]

area

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Urban	99	80.5	80.5	80.5
	Semi-Urban	10	8.1	8.1	88.6
	Rural	14	11.4	11.4	100.0
	Total	123	100.0	100.0	

Fig-6

Fig-6: Respondent distribution by area shows that urban residents predominate with 80.5%, while 8.1% were semi urban and 11.4% were rural. [1] Secondly, this urban centric demographic may impact the findings in regards to digital payment habits and access to technology.[2]

SPSS table results reveal a detailed analysis of consumer knowledge and awareness about digital payment systems, and the principal security threats and challenges confronting users. We present data that reveals how consumer perceptions of payment systems relate to their trust in those systems, and their attitudes towards security features crucial for understanding factors driving digital payment adoption. This paper seeks to help craft effective anti-fraud strategies that improve consumer confidence around safe use of digital payment methods.

Descriptive Statistics

	N Statistic	Mean Statistic	Std. Deviation Statistic	Kurtosis Statistic	Kurtosis Std. Error
familiar	123	4.07	.787	1.071	.433
understand	123	3.61	1.178	.417	.433
information	123	3.03	1.086	.316	.433
knowledge	123	3.61	1.178	.417	.433
termsandconditions	123	3.61	1.178	.417	.433
Valid N (listwise)	123				

Fig-7

Fig-7: Descriptive statistics show that respondents have a high level of familiarity with digital payment systems, with an average score of 4.07 that reflects people have a strong familiarity.[1] The mean scores in the understanding (3.61) and knowledge (3.61) questions however, do indicate that while consumers were aware, there could be a lag within their overall understanding and knowledge of the systems and the applicable terms and conditions, which scored exactly the same at 3.61.[2]

Descriptive Statistics

	N Statistic	Mean Statistic	Std. Deviation Statistic	Kurtosis Statistic	Kurtosis Std. Error
concern	123	4.53	.899	2.023	.433
security	123	2.46	1.210	.567	.433
onlinefraud	123	2.46	1.210	.567	.433
precautions	123	3.61	1.178	.417	.433
commonfraud	123	4.19	1.445	.257	.433
Valid N (listwise)	123				

Fig-8

Fig-8: Descriptive statistics show respondents' concern with digital payment security — with a mean score of 4.53 — indicates very high awareness of the risks. However, the mean score for security and online fraud awareness is indeed lower, at 2.46, suggesting that although consumers are worried, their understanding of particular security threats, or lack thereof, or past experiences with online fraud, can be lacking. Also, the mean value of the precaution taken has also been high that is 3.61 which show the moderate level of advanced behavioral barrier, which consumers apply while doing Digital Transactions.

Descriptive Statistics

	N Statistic	Mean Statistic	Std. Deviation Statistic	Kurtosis Statistic	Kurtosis Std. Error
securityfeatures	123	4.19	1.445	.257	.433
Howsatisfied	123	3.61	1.178	.417	.433
biometricauthenticatione	123	4.19	1.445	.257	.433
offersenhanced	123	4.19	1.445	.257	.433
passwordupdate	123	2.63	1.175	.123	.433
Valid N (listwise)	123				

Fig-9

Fig-9: Similarly, descriptive analysis using Microsoft Excel also shows that security features are well perceived in this digital payment system since the mean score is 4.19 indicated by the studied respondents' high confidence towards these security features as compared to the digital payment system. Moreover, consumers expressing satisfactory payment systems (mean=3.61), however, show a weaker engagement and proactivity with password updates (mean=2.63).

To assess the efficiency of the security awareness on the level of trust of consumers with the digital payments, the questionnaire survey includes the measure of trust questions

and the knowledge of the security in the payment system, and the attitudes towards security in the transaction processes, the intention of consumers to recommend use of the payment systems, and the frequency of reporting security incidents related to the payment systemBut one demographic question asks whether participants were active users of the tools in digital payments. Thus, this study aims at examining the extent of Security Awareness and usage of digital payments for receipt of information on the impact of Security perceptions on consumers.In this paper, we will consider the implications of this trend in conjunction with the level of digital payment adoption awareness.

In this analysis the concentration is on the correlation between the question asked to capture consumers' trust in digital payment systems, and consumers' frequency in utilizing digital payment solutions. That is why the study aims at applying the regression analysis to justify how higher levels of trust or security consciousness are associated with considerably higher levels of adoption of the digital payment methods.

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	7.886	1	7.886	211.115	<.001[b]
	Residual	4.520	121	.037		
	Total	12.407	122			

a. Dependent Variable: paymentmethod

b. Predictors: (Constant), trust

Fig-10

Fig-10: The results from the ANOVA table indicate a significant regression model (F value = 211.115, $p < 0.001$) which indicates that trust in digital payment systems can significantly predict choice of payment method.[1] Being able to explain a lot of the variance in payment method usage (total sum of squares 12.407),[2] the regression provides a very good explanation.

It studies how knowledge about security features in digital payment systems affects the frequent use of a particular digital payment type. The study then attempts to determine through regression analysis if increased awareness about the security features actually leads to an increase in digital transactions via digital payment systems and an increase in their trust of these payment systems.

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	7.886	1	7.886	211.115	<.001[b]
	Residual	4.520	121	.037		
	Total	12.407	122			

a. Dependent Variable: paymentmethod

b. Predictors: (Constant), awarenessofsecurityfeature

Fig-11

Fig-11: This shows us a very significant regression model with F value as 211.115 and p value less then 0.001, that is awareness of security features does matter in deciding the choice of payment mechanisms in consumers.[1] 12.407 is the total sum of squares indicating that the model accounts for a large part of the variance in the use of payment method.[2]

This analysis focuses on the relationship between consumers' perceived security when making digital payment and her/his frequency of using digital payment methods. The study attempts to measure whether increased usage of digital payment system is linked with heightened sense of security and hence the crucial role of security perceptions in directing the consumer behavior in the digital payment landscape through regression analysis.

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	7.886	1	7.886	211.115	<.001[b]
	Residual	4.520	121	.037		
	Total	12.407	122			

a. Dependent Variable: paymentmethod

b. Predictors: (Constant), feelsecure

Fig-12

Fig-12: ANOVA table shows a highly significant regression model, F value is 211.115 and $p < 0.001$, indicating that the digital payment perception makes the perception of feeling secure when making digital payment significantly influences the choice of digital payment.[1] This finding is important because it reaffirms the role of perceptions of security acting in digital transactions as a determinant on consumer behaviour.[2]

Then, the paper examines the relationship between associated digital payment system recommendations odds and related users awareness on the security characteristics of payment methods and the frequency of using these payment methods. For this reason, the study resorts to regression analysis in order to find out if the change in recommendation of and frequency of usage of digital payment systems by consumers owing to increased security awareness would close the gap between people's security perception and advertisement and behavior.

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	7.886	1	7.886	211.115	<.001[b]
	Residual	4.520	121	.037		
	Total	12.407	122			

a. Dependent Variable: paymentmethod

b. Predictors: (Constant), recommend

Fig-13

Fig-13: My regression model p value, F = 211.115, with a p value of < 0.001 was very significant showing that recommending digital payment systems does have a higher strength of association with digital payment systems frequency use. This finding demonstrates not only the powerful effect of security awareness on consumer controlled digital payment behavior, but also the important role of consumer advocacy.

In this analysis, we study the correspondence between how often people use digital payment methods versus how people communicate digital payment security.Using regression analysis, the study seeks to determine whether discussions of security experiences in digital payment contribute to the adoption and frequency of digital payment use, refocusing on how social interaction influences

consumer behavior in the digital payment environment.

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	5.628	1	5.628	100.464	<.001[b]
	Residual	6.778	121	.056		
	Total	12.407	122			

a. Dependent Variable: paymentmethod

b. Predictors: (Constant), shareyourexperiences

Fig-14

Fig-14: An ANOVA table shows an extremely significant model, with an F of 100.464 and a p<.001, which suggests that the frequency with which people share experiences of digital payment security is a very good predictor of the usage of digital payment methods.[1] This highlights how interaction among people is linked to a customer's behavior in the digital payment arena[2].

This study underpins the decisiveness of security awareness in determining behaviour of consumers in India's current digital payment ecosystem. Using digital payment systems is influenced by the likelihood of users to recommend digital payment systems and frequency of experience sharing about digital payment security. However, the significance levels of the two regression models in ANOVA result are less than 5% which results in rejecting null hypothesis of both regression models (H0). The results of this study suggest that perception of security, trust in payment system, and online fraud experience are indeed determinants of consumer choice of payment method.

The online survey reveals the data collected which indicates that consumers have an overwhelming focus on security when making a decision. A digital first mindset among consumers is not fostered unless the confidence in the payment framework is high and, correspondingly, was reflected by the fact that respondents reporting higher trust in digital payment systems were more likely to adopt these methods. This finding is consistent with the existing literature on a driver of adoption of new technologies, trust. Moreover, the research shows that bad online fraud experience can dissuade consumers to make use of digital payment modes especially the type of the transaction involved. The fact that security and fraud are numerous worries that need addressing with targeted educational campaigns underscores this inconsistency in behavior.

V. Conclusion

This study concludes by discussing the role of security awareness in giving power in the hands of consumers in India's digital payment ecosystem. Perception and trust play a key role in digital payment adoption, and hence financial institutions and governments have to present consumer education on security measures as top priority. This will be crucial to encourage wider adoption across the digital payment landscape, as it continues to evolve and become both more widely used and more widely sought-after — bringing with it a need to address increasingly prevalent issues of online fraud and increasing levels of consumer confidence. The two sides of cash and consumers' payment preferences comprise of customers who have payment preferences in the realms of cash and digital payments, both of which are important but worthy of being equally understood, both of the technological front and of the factors that govern product choices. Implementation of targeted awareness campaigns and robust security protocol along with concerted efforts can bring an environment of more secure and safe for the people and development conducive to its economic growth in India.

References :

[1] Singhal, A.(2021)."The Rise of Digital Payment Systems in India: They key theme that emerged for both opportunities and challenges is Opportunities and Challenges. This paper is published and can be accessed in the Journal of Financial Technology 5(2),pp 45-60

[2] Sujith, S., & J. C., P. (2017)."Consumer Adoption of Digital Payment Systems: A Study of Indian Consumers." International Journal of Business and Management Invention, 6(11),1-10.

[3] Fernandes, A. (2013)."Cyber Fraud in Digital Payments: Consumer Trust: An Analytical Framework." In: Indian Journal of Marketing, 43 (6), pp. 12-20.

[4] Neha Priya, & J. A. (2021)."Understanding the Security Features of Digital Payment Systems: A Consumer Perspective." International Journal of Information Management*, 57, 102–110.

[5] Gupta, R, & R.K (2020). Consumer Attitude Towards Digital Payment Systems: A Study in India. Volume 55 Journal of Retailing and Consumer Services, 102-110.

[6] Ruangmei, K., & Gethe, A. (2023)."Digital Payment Adoption in Rural India: Barriers and Opportunities." Journal of Rural Studies , vol 89, pp 45 – 55

[7] Deng, Y., & N.R. (2019)."Phishing Scams and Identity Theft: Security Awareness: The Role Security Awareness. Computers & Security, 85, pp. 123-130.

[8] Chang, L., & L.M. (2022). Cybersecurity Awareness and Its Relation to Digital Payment Acceptance. Vol. 1 Issue 2: pp. 1-15 Journal of Cybersecurity and Privacy.

[9] Rama Vedashree, & Nath Parameshwaran. (2020)."Empowering Consumers Through Security Awareness: Digital Payment Systems: A Literature Review for the Article "A Study of Digital Payment Systems."Journal of Financial Services Marketing*, 25(3), 215-225.

[10] Shree, S., & B. P. (2021)."Trust and Consumer Behavior in Digital Payment Systems: Consumers' Attitude towards Point-Of-Purchase Advertising: An Empirical Study.International Journal of Consumer Studies,45(4), 456- 467.