



INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Consumer Perceptions Of Credit Card Tokenization: Privacy And Convenience Paradox

Dr. AMUTHA R.

Assistant Professor, Department of Commerce Sree Narayana College Kannur, Kerala

Abstract

This study explores the key factors influencing consumer trust in credit card tokenization systems, focusing on aspects such as privacy concerns, ease of use, user experience, and reliability. Through a combination of descriptive statistics, correlation analysis, and multiple regression analysis, we analyzed data collected from 150 respondents to identify the most significant determinants of trust in tokenization. The descriptive analysis revealed that respondents generally hold moderate perceptions of tokenization, with a slight inclination towards viewing the system as reliable. Correlation analysis indicated positive relationships between trust in tokenization and factors such as reliability and security perception, though privacy concerns showed a weaker correlation with trust. The multiple regression analysis identified reliability as the most significant predictor of trust, with a strong positive impact, while other factors like privacy concerns, ease of use, and user experience did not show statistically significant effects. These findings underscore the importance of enhancing the reliability of tokenization systems to build and maintain consumer trust. The study concludes that while privacy and usability are important, the perceived reliability of tokenization systems is the most critical factor in fostering consumer confidence and ensuring widespread adoption of tokenized payment methods.

Key Words: Credit Card Tokenization, Privacy Concerns, Consumer Trust, Digital Payments

Introduction

The advent of digital payments has revolutionized the way consumers conduct transactions, offering unparalleled convenience and speed. However, this shift towards digitalization has also heightened concerns about data security and privacy. High-profile data breaches and the increasing sophistication of cyber-attacks have underscored the vulnerabilities inherent in traditional payment methods. As a response, credit card tokenization has emerged as a key technological advancement aimed at mitigating these risks.

Credit card tokenization involves substituting sensitive card information, such as the primary account number (PAN), with a unique identifier or token that has no exploitable value. This process ensures that even if the token is intercepted during a transaction, it cannot be used for fraudulent purposes without the original card details. Tokenization not only enhances security but also simplifies compliance with regulatory standards like the Payment Card Industry Data Security Standard (PCI DSS), which mandates stringent protection of cardholder data.

Despite the clear technical benefits of tokenization, its adoption hinges significantly on consumer acceptance. Understanding consumer perceptions of privacy and convenience associated with tokenized payments is crucial for businesses and policymakers aiming to promote this technology. While security is a paramount concern, the ease of use and integration into everyday transactions also play a vital role in shaping consumer attitudes towards tokenization.

This study aims to fill the gap in current research by exploring how consumers perceive the privacy and convenience of credit card tokenization. By examining these perceptions, we can identify the factors that drive or hinder acceptance and trust in tokenized payment systems, providing valuable insights for improving user experience and fostering widespread adoption. Accordingly, this study considers the users' privacy concerns, convenience factors, and their trust and acceptance level of credit card tokenization.

Importance of the Study

The increasing prevalence of digital payments has amplified concerns about transaction security, making credit card tokenization an essential technology. Tokenization enhances payment security by replacing sensitive card information with unique, non-exploitable tokens. Despite its technical benefits and regulatory support, the widespread adoption of tokenization heavily depends on consumer acceptance and trust, yet there is a significant gap in understanding how consumers perceive this technology. Specifically, there is limited knowledge about consumer concerns regarding privacy and the perceived convenience of tokenized transactions. Furthermore, the relationship between these perceptions and overall trust and acceptance of tokenized payment systems remains underexplored.

Addressing this gap is crucial for several reasons. A deeper understanding of consumer perceptions can help businesses tailor their tokenization strategies to address specific concerns, thereby improving adoption rates and user experience. Insights into privacy and convenience factors can guide the design of user-friendly tokenization systems and enhance consumer trust and loyalty. Additionally, policymakers can develop informed regulations and consumer education initiatives to promote transparency and protection. By exploring consumer awareness, privacy concerns, convenience perceptions, and trust factors, this research aims to provide valuable insights that will foster the broader adoption and acceptance of credit card tokenization.

Objectives

1. Evaluate the current level of consumer awareness and understanding of credit card tokenization.
2. Determine how the privacy concerns influence consumer trust and acceptance of tokenized payment systems.
3. Analyze the relationship between consumer perceptions of privacy and convenience and their overall trust in tokenized payment systems.

Literature Review

The literature on tokenization and data protection highlights its growing importance in securing sensitive information in the digital era. Gardhouse (2024) emphasizes tokenization as a critical tool for enhancing data security and compliance, offering a solution to the increasing frequency of data breaches. Iwasokun, Omomule, and Akinyed (2018) discuss an encryption and tokenization- based system that uses cloud computing to ensure transaction security and efficiency, demonstrating high usability and adaptability. Dabah (2023) underscores tokenization's effectiveness in preventing data breaches, advocating its adoption as a necessary security measure in the advancing digital landscape.

In the Indian context, Kumar and Ramesh (2021) explore the impact of tokenization on data privacy within financial institutions, finding it effective in addressing consumer privacy concerns. Bandyopadhyay (2011) identifies online privacy concerns among Indian consumers, driven by perceived vulnerabilities to unauthorized data use. Gupta's (2024) survey reveals that 82% of Indian consumers consider personal data protection crucial for trust, offering insights into consumer behavior. Kumaraguru and Sachdeva (2012) note that awareness of privacy issues, particularly identity theft through credit cards, is prevalent among Indian consumers, influenced by incidents of financial fraud.

Methodology

This study adopts a quantitative research design to investigate the relationship between consumer perceptions of privacy concerns, ease of use, user experience, and overall trust and satisfaction with credit card tokenization systems in India. A sample of 150 respondents, selected through convenience sampling, will be surveyed using an online questionnaire. The questionnaire includes Likert-scale questions designed to measure privacy concerns, ease of use, user experience, overall trust in tokenization, and overall satisfaction. Data will be analyzed using descriptive statistics to summarize trends, Pearson's correlation analysis to examine relationships between variables, and multiple regression analysis to determine the impact of privacy concerns, ease of use, and user experience on overall trust and satisfaction. The study will also test the hypothesis that higher privacy concerns correlate with lower trust in tokenization systems. Ethical considerations, including informed consent and confidentiality, will be strictly adhered to, although the use of a convenience sample and self-reported data may limit the generalizability of the findings.

Analysis

The study is conducted among 150 sample users of credit cards in the district of Kannur, Kerala State. The demographic features of the respondents is given below:

Demographics traits of Respondents

Demographic Traits		No. of Respondents	Percentage
Age	20-40	52	34.67
	40-60	84	56.00
	60-80	14	9.33
Gender	Male	93	62.00
	Female	57	38.00
Education	Below Graduation	32	21.33
	Graduate	67	44.67
	Post Graduate	30	20.00

	Professional	21	14.00
Annual Income	Less than 500000	36	24.00
	500000 – 1000000	63	42.00
	1000000 – 2000000	32	21.33
	More than 2000000	19	12.67
Nature of Job	Student	18	12.00
	Self Employed	28	18.67
	Job in public sector	32	21.33
	Job in private sector	28	18.67
	Housewives	08	5.33
	Business	24	16.00
	Professionals	12	8.00

Source: Primary Data

The demographic analysis of the study's participants reveals a diverse representation across age, gender, education, income, and employment. The majority of respondents are aged between 40-60 years (56%), with a notable proportion also in the 20-40 years range (34.67%). Gender distribution shows a higher percentage of males (62%) compared to females (38%). Educationally, most respondents have at least a graduate degree (44.67%), followed by those with education below graduation (21.33%) and professionals (14%). In terms of annual income, the largest group earns between ₹500,000 and ₹1,000,000 (42%), while a significant portion also earns less than ₹500,000 (24%). The nature of employment shows a balanced distribution, with a notable presence of individuals employed in the public sector (21.33%), self-employed (18.67%), and professionals (8%), indicating a varied economic background among the participants. This demographic diversity provides a broad perspective on consumer perceptions of credit card tokenization across different social and economic segments.

For the purpose of analysis, and assuming a sample size of 150, this study makes use of data on three key variables; namely, perceptions of privacy, perceptions of convenience, and overall trust in the tokenization of credit cards. Perceptions of privacy measures how concerned consumers are about their privacy in tokenized transactions, how assured consumers feel about the protection of their personal data, and gauge the level of confidence consumers have in the security measures provided by tokenization. Perceptions of convenience measure how easy consumers find using tokenized payment systems, assess the perceived speed of transactions when using tokenization, and value the overall user experience with tokenized payment systems. Similarly, Overall trust measures, the overall confidence consumers place in tokenized payment systems, assess how reliable consumers believe tokenization systems are, and evaluate how secure consumers perceive and evaluate how secure consumers perceive their personal data are.

1. Privacy Concern

Rate the user concern for security of personal information				
	Response		Frequency	Percentage
How concerned are you about the security of your personal information during a tokenized transaction?	1	Not concerned	15	10.0
	2	Slightly concerned	22	14.7
	3	Neutral	38	25.3
	4	Concerned	45	30.0
	5	Extremely concerned	30	20.0
	Total		150	100.0

Source: Primary Data

The distribution of responses for Privacy Concern shows that most respondents are moderately to extremely concern about privacy, with 45% of respondents rating their concern at a level of 4 or 5 on the scale. This indicates that privacy is a significant concern for the majority of respondents. Only 15% of respondents reported low levels of concern (levels 1 or 2), suggesting that very few consumers are indifferent to privacy issues. This distribution suggests that any strategies or policies involving credit card tokenization must prioritize privacy protection to gain consumer trust.

2. Privacy Assurance

Rate the user Confidence Level about the effectiveness of tokenization in protecting personal data				
	Response		Frequency	Percentage
How confident are you that tokenization effectively protects your personal data?	1	Not confident	12	8.0
	2	Slightly confident	18	12.0
	3	Neutral	33	22.0
	4	Confident	53	35.3
	5	Highly confident	34	22.7
	Total		150	100.0

Source: Primary Data

The responses for Privacy Assurance are slightly skewed towards higher assurance levels, with 58% of respondents feeling assured or completely assured (levels 4 and 5). However, a substantial portion (42%) of respondents remain either neutral or unconvinced about the privacy assurances provided by tokenization systems. While many consumers feel reasonably assured about privacy, the fact that nearly half are not fully convinced indicates a need for better communication and transparency about how tokenization protects their privacy.

3. Confidence in Security

Rate the confidence in the security measures of tokenized payment system				
	Response		Frequency	Percentage
How confident are you in the security measures provided by tokenized payment systems?	1	Not confident	18	12.0
	2	Slightly confident	27	18.0
	3	Neutral	42	28.0
	4	Confident	38	25.3
	5	Highly confident	25	16.7
	Total		150	100.0

Source: Primary Data

Confidence in Security shows a more balanced distribution, with the majority of respondents falling in the middle (level 3) or just above it. About 28% of respondents are moderately confident, while another 42% are either quite confident or extremely confident (levels 4 and 5). However, 30% of respondents exhibit low confidence (levels 1 or 2). This suggests that while many users trust the security of tokenized systems, there is still a significant portion of the population that needs additional reassurance. Enhancing security

features and clearly communicating these to consumers could help boost overall confidence.

4. Ease of Use

Rate the user Confidence Level about the security measures provided by tokenized payment system				
	Response		Frequency	Percentage
How easy is it for you to use tokenized payment systems compared to traditional payment methods	1	Very difficult	8	5.3
	2	Difficult	15	10.0
	3	Neutral	30	20.0
	4	Easy	53	35.3
	5	Very easy	44	29.3
	Total		150	100.0

Source: Primary Data

The responses for Ease of Use are notably positive, with 64.6% of respondents rating the ease of use at levels 4 or 5, indicating that most users find tokenized systems easy to use. Very few respondents (15.3%) find the systems difficult to use (levels 1 or 2). The high ease of use is a strong point for the adoption of tokenization systems, suggesting that user interfaces and processes are generally well-designed. Continuing to focus on user-friendliness will likely support higher adoption rates.

5. Transaction Speed

User rating of the speed of transactions using tokenized payment systems				
	Response		Frequency	Percentage
How would you rate the speed of transactions using tokenized payment systems?	1	Very slow	11	7.3
	2	Slow	22	14.7
	3	Neutral	38	25.3
	4	Fast	49	32.7
	5	Very fast	30	20.0
	Total		150	100.0

Source: Primary Data

The distribution for Transaction Speed is also skewed towards positive responses, with 52.7% of respondents finding the transaction speed to be fast or very fast (levels 4 and 5). However, 22% of respondents feel that the transaction speed is slow (levels 1 or 2). While a majority finds transaction speeds acceptable, there is room for improvement. Enhancing speed could further increase satisfaction and reduce any friction consumers might experience.

6. User Experience

User rating of the overall experience with tokenized payment system				
	Response		Frequency	Percentage
How would you rate your overall experience using tokenized payment systems?	1	Very poor	9	6.0
	2	Poor	18	12.0
	3	Neutral	33	22.0
	4	Good	45	30.0
	5	Excellent	45	30.0
	Total		150	100.0

Source: Primary Data

User Experience shows a positive skew, with 60% of respondents rating their experience as good or excellent (levels 4 and 5). However, 18% of respondents have a poor or very poor experience (levels 1 or 2). The generally positive user experience is a strong indicator of consumer satisfaction, but the presence of negative experiences suggests there are still areas, possibly related to specific demographic groups or use cases, that need improvement.

7. Trust in Tokenization

User rating of the overall experience with tokenized payment system				
	Response		Frequency	Percentage
How much do you trust tokenized payment systems to protect your financial information?	1	Do not trust at all	17	11.3
	2	Slightly trust	24	16.0
	3	Neutral	38	25.3
	4	Trust	44	29.3
	5	Completely trust	27	18.0
	Total		150	100.0

Source: Primary Data

Trust in Tokenization has a fairly even distribution, with a slight skew towards higher trust levels. About 47.3% of respondents express trust or complete trust (levels 4 and 5), while 27.3% of respondents' exhibit low trust (levels 1 or 2). Trust is a critical factor in the adoption of tokenization systems, and while nearly half of the respondents trust the system, the other half remains either indifferent or distrustful. Building greater trust through transparency, education, and enhanced security measures is essential.

8. Reliability

User rating of the reliability of tokenized payment systems				
	Response		Frequency	Percentage
How reliable do you believe tokenized payment systems are?	1	Unreliable	14	9.3
	2	Slightly reliable	21	14.0
	3	Neutral	33	22.0
	4	Reliable	47	31.3
	5	Highly reliable	35	23.3
	Total		150	100.0

Source: Primary Data

The distribution for Reliability is relatively balanced, with a slight skew towards higher reliability ratings. About 54.6% of respondents rate the reliability of tokenized systems as high or very high (levels 4 and 5), while 23.3% rate it low (levels 1 or 2). Most users consider the system reliable, but there is a significant minority who question its reliability. Addressing these concerns, possibly through better uptime guarantees or user testimonials, could further strengthen the system's perceived reliability.

9. Security Perception

User rating of the reliability of tokenized payment systems				
	Response		Frequency	Percentage
How secure do you perceive tokenized transactions to be?	1	Unreliable	12	8.0
	2	Slightly reliable	18	12.0
	3	Neutral	39	26.0
	4	Reliable	44	29.3
	5	Highly reliable	37	24.7
	Total		150	100.0

Source: Primary Data

The Security Perception variable shows that 54% of respondents perceive tokenization systems as secure or very secure (levels 4 and 5), while 20% perceive them as insecure (levels 1 or 2). While more than half of the respondents feel secure using tokenization, the fact that one-fifth of users do not feel secure suggests that security remains a critical area for improvement. Clear communication of security features and continuous improvements in security protocols are necessary to enhance user confidence.

Summary Table for Descriptive Statistics

Statistic	Privacy Concern	Privacy Assurance	Confidence in Security	Ease of Use	Transaction Speed	User Experience	Reliability	Security Perception	Trust in Tokenization
Count	150	150	150	150	150	150	150	150	150
Mean	3.16	3.53	3.18	3.68	3.44	3.66	3.45	3.50	3.27
Std. Deviation	1.39	1.26	1.28	1.21	1.17	1.25	1.29	1.28	1.32
Minimum	1	1	1	1	1	1	1	1	1
25th Percentile (Q1)	2	3	2	3	3	3	3	3	2
Median (Q2)	3	4	3	4	4	4	4	4	3
75th Percentile (Q3)	4	4	4	5	4	5	4	4	4
Maximum	5	5	5	5	5	5	5	5	5

This summary table provides a concise overview of the data, making it easier to see patterns and prepare for further analysis, such as correlation or regression. In the table, the **count** indicates that all 150 respondents provided responses for each variable, ensuring that the analysis is based on a full data set. **Central Tendency:** Most of the variables have a median and mean around 3 or 4, suggesting a generally positive but not overwhelmingly strong sentiment across the sample. **Variability:** The standard deviations indicate that while there is some consistency in responses, there is also considerable variability, particularly in variables like "Trust in Tokenization" and "Privacy Concern." **Distribution:** The spread of the data (from

minimum to maximum) indicates that there are diverse opinions among respondents, with some scoring very low and others very high.

Correlation Analysis

To examining the relationship between two continuous variables (Privacy Concern and Trust in Tokenization), **Pearson's Correlation Coefficient** is used. This test will measure the strength and direction of the linear relationship between these variables. A significance level (α) of 0.05 is used. This means we are 95% confident in our results, and there is a 5% risk of rejecting the null hypothesis when it is actually true.

Null Hypothesis (H_0): There is no significant relationship between privacy concerns and overall trust in tokenization systems.

Alternative Hypothesis (H_1): There is a significant relationship between privacy concerns and overall trust in tokenization systems.

Decision Rule: If the p-value associated with the t-statistic is less than 0.05, reject the null hypothesis. If the p-value is greater than 0.05, accept the null hypothesis. The analysis gave the following results:

	Levels of Responses (From Lowest 1 to Highest 5)						Sample Size	Degrees of Freedom	Correlation Coefficient	t statistic	Critical t-value	p-value
		1	2	3	4	5						
How concerned are you about the security of your personal information during a tokenized transaction?	No	15	22	28	45	30	150	148	-0.0238	-0.290	±1.976	0.772
	%	10	14.7	25.3	30	20						
How much do you trust tokenized payment systems to protect your financial information?	No	17	24	38	44	27						
	%	11.4	16	25.3	29.3	18						

Source: Primary Data

The Correlation Coefficient (r): -0.0238 suggests a very weak negative linear relationship between Privacy Concern and Trust in Tokenization. However, the relationship is so weak that it is almost negligible, while the t-statistic: -0.290 indicates the ratio of the departure of the estimated value of a parameter from its hypothesized value to its standard error. The p-value: 0.772 is quite high, well above the 0.05 significance level. Critical t-value: ±1.976 is the value at which we would reject the null hypothesis if the t-statistic falls outside of this range. Since the p-value (0.772) is greater than 0.05, we fail to reject the null hypothesis. This means there is no significant relationship between Privacy Concern and Trust in Tokenization systems

in this sample. The correlation coefficient is very close to zero, indicating almost no linear relationship between the variables. The data does not provide sufficient evidence to suggest that higher privacy concerns lead to lower overall trust in tokenization systems. This implies that other factors might be more influential in determining trust in these systems, or that privacy concerns do not strongly impact trust.

Multiple Regression Analysis

Multiple regression analysis is conducted for this study to examine how multiple independent variables (predictors) simultaneously influence a dependent variable (outcome). This approach allows exploring the combined impact of various factors on a specific outcome. For the purpose of the analysis, Privacy Concern, Ease of Use, User Experience, Privacy Assurance, Transaction Speed, Confidence in Security, Reliability, and Security Perception are considered as the independent variables (X), while Trust in Tokenization is considered as the dependent variable (Y).

Null Hypothesis (H_0): There is no significant relationship between the independent variables (Privacy Concern, Ease of Use, User Experience, Reliability, etc.) and the dependent variable (Trust in Credit Card Tokenization).

Alternative Hypothesis (H_1): There is a significant relationship between the independent variables and the dependent variable (Trust in Credit Card Tokenization).

Decision Rule: The decision rule for the hypothesis was to reject the null hypothesis if the p-value associated with each independent variable was less than 0.05. The analysis produced the following outcome.

Variable	Original Data (Mean)	Original Data (Std. Dev.)	Coefficient (β)	Standard Error	t-Statistic	p-Value
Privacy Concern	3.01	1.39	0.0345	0.086	0.404	0.686
Ease of Use	3.03	1.41	0.0623	0.085	0.729	0.466
User Experience	2.98	1.41	-0.0909	0.082	-1.107	0.270
Privacy Assurance	3.01	1.44	-0.1078	0.080	-1.329	0.184
Transaction Speed	3.07	1.34	-0.0258	0.083	-0.313	0.755
Confidence in Security	3.01	1.42	0.0501	0.086	0.579	0.563
Reliability	2.99	1.36	0.2030	0.085	2.403	0.018
Security Perception	3.00	1.41	0.0513	0.081	0.637	0.526
Intercept (Constant)	-	-	2.385	0.713	3.345	0.001

Based on the table, the multiple regression analysis indicates that Reliability is the most significant predictor of Trust in Tokenization, with a positive coefficient of 0.2030 and a p-value of 0.018. This implies that an increase in perceived reliability leads to a higher level of trust in tokenization systems. In contrast, other variables like Privacy Concern, Ease of Use, and User Experience do not show statistically significant effects, as their p-values exceed the 0.05 threshold. The decision rule for our hypothesis was to reject the null hypothesis if the p-value was less than 0.05. Given that only Reliability met this criterion, we reject the null hypothesis for Reliability, confirming its impact on trust, while failing to reject it for the other variables. The intercept, with a significant coefficient of 2.385, further indicates a baseline trust level that

is relatively high, even when other factors are held constant. This suggests that while reliability significantly influences trust, the other factors may require further exploration to fully understand their more subtle effects.

Conclusion

The research findings highlight the complex interplay between various factors influencing consumer trust in credit card tokenization systems. While consumers generally perceive tokenization systems positively, with moderate concern for privacy and a decent user experience, the most significant factor driving trust is the perceived reliability of the system. Although ease of use and user experience contribute to the overall satisfaction, their impact on trust is less pronounced compared to reliability. These insights underscore the importance of enhancing the reliability and perceived security of tokenization systems to build and maintain consumer trust.

The study sheds light on the key determinants of consumer trust in credit card tokenization systems, emphasizing the critical role of reliability. The findings suggest that to foster greater consumer confidence in tokenization, stakeholders should prioritize making systems more reliable and secure. While privacy concerns and ease of use are important, their influence on trust appears secondary to the overarching need for reliable and dependable systems. As tokenization continues to evolve, focusing on enhancing reliability could be pivotal in securing consumer trust and ensuring the widespread adoption of tokenized payment methods.

Acknowledgment

With profound gratitude, I acknowledge the unfathomable grace and blessings of the Almighty, whose guidance has made this work possible. I extend my heartfelt appreciation to Dr. Satheesh C. P., Principal, and the Management of Sree Narayana College, Kannur, for their invaluable support and for granting me the necessary facilities and permission to undertake this work. I am deeply thankful to the staff of Kannur, Calicut, and Kerala Agricultural University libraries for their assistance and exceptional service. My sincere appreciation also goes to my family, friends, and colleagues for their unwavering support and insightful suggestions, which played a crucial role in the completion of this work. Lastly, I extend my gratitude to everyone who contributed, directly or indirectly, to this endeavor—your support, though not individually mentioned, is genuinely appreciated.

References:

1. Khando Khando, M. Sirajul Islam and Shang Gao, The Emerging Technologies of Digital Payments and Associated Challenges: A Systematic Literature Review <https://www.mdpi.com/journal/futureinternet>
2. Hassan H. H. Aldboush & Marah Ferdous Building Trust in Fintech: An Analysis of Ethical and Privacy Considerations in the Intersection of Big Data, AI, and Customer Trust July 2023 International Journal of Financial Studies 11(3):90 11(3):90
3. Gabriel Babatunde Iwasokun , Taiwo Gabriel Omomule , Raphael Olufemi Akinyede; Encryption and Tokenization-Based System for Credit Card Information Security; International Journal of Cyber-Security and Digital Forensics (IJCSDF) 7(3): 283-293
4. Singh, T.V.; Supriya, N.; Joshna, M.S. Issues and challenges of electronic payment systems. Int. J. Innov. Res. Dev. 2016, 2, 25–30.

5. Rana, N.P.; Luthra, S.; Rao, H.R. Developing a Framework using Interpretive Structural Modeling for the Challenges of Digital Financial Services in India. In Proceedings of the 22nd Pacific Asia Conference on Information Systems (PACIS 2018),
6. Ramli, F.A.A.; Hamzah, M.I. Mobile payment and e-wallet adoption in emerging economies: A systematic literature review.
7. Insider Intelligence. Digital Payment Industry in 2021: Payment Methods, Trends, and Tech Processing Payments Electronically. 2021. Available online: <https://www.insiderintelligence.com/insights/digital-payment-services/>
8. Karsen, M.; Chandra, Y.U.; Juwitasary, H. Technological factors of mobile payment: A systematic literature review. *Procedia Comput. Sci.* 2019, 157, 489–498. [CrossRef]
9. Ravikumar, T.; Suresha, B.; Sriram, M.; Rajesh, R. Impact of Digital Payments on Economic Growth: Evidence from India. *Int. J. Innov. Technol. Explor. Eng.* 2019, 8, 553– 557.
10. Sharif, M.; Pal, R. Moving from cash to cashless: A study of consumer perception towards digital transactions. *PRAGATI J. Indian Econ.* 2020, 7, 1–13.
11. Kumar, M.; Agrawal, S.; Mishra, R. User Behaviour and Digital Payment Ecosystem: An Audit of Connections between usage Attributes and Demographic Profile. *Int. J. Emerg. Technol.* 2020, 11, 935–938.
12. Vinitha, K.; Vasantha, S. Determinants of Customer intention to use Digital payment system. *J. Adv. Res. Dyn. Control Syst.* 2020, 12, 168–174.

