



BUILDING TRUST IN DIGITAL PAYMENTS: THE ROLE OF CYBERSECURITY ASSURANCE IN OVERCOMING CONSUMER SKEPTICISM

Javeria Iqbal¹, Muhammad Hafeez², Ahras Rashid³, Zainab Tayyab⁴

¹Institute of Business Management Sciences, University of Agriculture, Faisalabad, Pakistan.

²Institute of Business Management Sciences, University of Agriculture, Faisalabad, Pakistan.

Email: Muhammad.Hafeez@uaf.edu.pk

³Institute of Business Management Sciences, University of Agriculture, Faisalabad, Pakistan.

⁴Institute of Business Management Sciences, University of Agriculture, Faisalabad, Pakistan

KEYWORDS	ABSTRACT
Cybersecurity Assurance, Digital Payment, Institutional Trust, Consumers, Generation Z.	The growing use of digital payment technologies has significantly changed the way consumers carry out financial transactions. This shift is particularly evident among Generation Z, who are generally more comfortable with digital technologies and increasingly prefer cashless payment methods. However, despite the rapid expansion of digital payment services, concerns regarding security, privacy, fraud, and trust remain important factors that may discourage users from fully adopting these technologies. Much of the existing research on digital payment adoption has focused on factors such as perceived usefulness, ease of use, convenience, and technology acceptance. Comparatively less attention has been given to how cybersecurity assurance and Institutional Trust can reduce users' concerns and strengthen their confidence in digital payment systems. This issue is particularly relevant in Pakistan, where the digital payment ecosystem is expanding rapidly, yet users may still have concerns about the security of their financial information, the reliability of digital platforms, and the institutions responsible for providing these services. Therefore, this paper aims to assess the Cybersecurity Assurance and Institutional Trust on Digital Payment Usage among Generation Z consumers in Pakistan. Understanding these relationships can provide valuable insights into how security measures and trust in financial institutions shape consumers' willingness to use digital payment services. The findings may help fintech companies, banks, and other financial institutions better understand the factors that influence digital payment behavior and develop strategies that improve users' confidence in their services. In particular, stronger cybersecurity practices, transparent security mechanisms, and greater institutional credibility may help address users' concerns and encourage more frequent use of digital payment platforms. By examining these factors within the Pakistani context, the study addresses an area that has received relatively limited attention in the existing literature and contributes to a broader understanding of digital payment adoption among Generation Z. The findings may also provide useful recommendations for policymakers and regulatory authorities seeking to strengthen cybersecurity standards, promote institutional trust, and develop a safer, more reliable, and inclusive digital payment ecosystem in Pakistan.
ARTICLE HISTORY	 2026 Journal of Social Research Development
Date of Submission: 20-09-2026	
Date of Acceptance: 10-10-2026	
Date of Publication: 13-10-2026	
Correspondence	
Email:	Muhammad.Hafeez@uaf.edu.pk
DOI	https://doi.org/10.59075/jsrd.v7i8.596
Volume/Issue	7(8), 2026, 411-433

Background

In recent two decades, several global financial systems have changed, particularly with the removal of cash and the replacement of face-to-face banking with digital financial systems. The merging of several technologies such as AI, the Internet, and FinTech created different opportunities for people to interact with the financial system and changed the way people transact financially. For example, digital payment systems have allowed consumers to shop and conduct financial transactions without the need to visit a physical branch of a financial institution. Additionally, digital payment systems have created convenience for users to pay for goods and services anywhere and at any time. Digital payment systems have facilitated economic activities and contributed to the growth of economies (Fortes & Rita, 2016).

COVID-19 also propelled changes in the financial systems to increase the use of contactless payment systems, e-commerce and online banking. Digital payment systems also facilitated financial transactions in developing countries by providing cross border and borderless payment systems and surpassing geographical boundaries where people do not have access to sufficient financial institutions. Digital payment systems allowed users to make payment transactions anywhere and at any time. The best example of such systems is RAST in Pakistan, where other digital payment systems such as JazzCash, Easypaisa, Nayapay and Sadapay experienced rapid growth, especially among the youth.

While the financial sector is currently undergoing a period of significant change, the shift away from cash transactions to digital payments has only just begun. One of the main reasons people are hesitant to use digital payments is the risk of a cyber attack, bank fraud, or identity theft. To address these concerns, greater confidence is required of the general public in the security and reliability of the digital financial systems on which they will be relying. In the case of less developed countries, these challenges are compounded by the emerging cybersecurity threats, legal defenses, and levels of digital awareness (Awan et al., 2019; Ahmed et al. 2024).

While digital technology is widely used by the youth of today, specifically by the members of Generation Z (born between 1997 and 2012), this does not mean they automatically trust digital payments. Young consumers are rightly concerned with the vulnerability of their financial and personal information, and the reliability of the digital platforms on which they will be transacting. Careful consideration is given by young consumers before financial transactions (Schrack, 2024).

Digital payments systems' ability to secure customers' financial transactions, personal information and data determines customers' levels of confidence in adopting digital payments systems. There are several options to mitigate perceived risks. There are a range of user authentication methods and features including, but not limited to, encryption, biometrics, multi-factor authentication, one-time passwords, secure servers, transaction alerts, and monitoring systems (Khan et al., 2023). The integration of these features signal to customers that financial institutions are safe to do business with and that consumers will not be defrauded.

Institutional trust serves a similar purpose as cybersecurity assurance. Consumers believe that certain banking and financial services institutions are responsible and reliable in protecting their interests and will not act in a way detrimental to the consumers' interests. There are several ways to gain consumers' trust including high-quality service, positive user experience, effective customer support, complaint resolution, and refunds (Poerjoto et al., 2021). It has also been found that consumers trust traditional banking and financial services institutions, and as such, it positively affects customers' confidence in traditional banking and financial services institutions' digital offerings (Yu et al., 2018).

Cybersecurity assurance and institutional trust are linked. Positive user experience and trust act as a bridge for adoption of digital payment systems (Riaz et al., 2025). Technical safeguards alone may be insufficient when consumers distrust institutions, while institutional reputation may have limited influence when digital systems are perceived as insecure.

Although previous research has widely explored digital payment adoption using theories such as the Technology Acceptance Model (TAM) and the Theory of Planned Behavior (TPB), relatively little attention has been given to the combined role of Cybersecurity Assurance and Institutional Trust in shaping Digital Payment Usage among Generation Z consumers in Pakistan. To address this gap, the present study examines how cybersecurity assurance and trust in financial institutions can reduce consumers' concerns and hesitation toward digital financial services and encourage greater use of digital payment platforms. The findings are expected to help banks, fintech companies, and other financial institutions strengthen their cybersecurity practices while building greater confidence among consumers. In addition, the study may provide useful insights for policymakers and regulatory authorities in developing effective cyber regulations, improving consumer and financial protection, and promoting greater financial inclusion in Pakistan.

Study Importance

The study has important implications for policymakers and regulatory authorities, particularly the State Bank of Pakistan. It highlights the need for effective cybersecurity regulations and consumer protection measures to strengthen public trust in digital financial services. The findings can help banks and fintech companies identify areas where greater attention is needed to improve the security of their digital platforms, provide better customer experiences, and maintain transparency in their services. Such improvements may help strengthen consumer confidence and encourage the wider use of digital payment systems.

The findings may further support efforts to stimulate financial inclusion by creating a safer and more trustworthy digital payment environment. From an academic perspective, the research will contribute by providing further evidence on the role of cybersecurity and institutional trust in shaping digital payment usage, particularly context of Pakistani Generation Z consumers.

Problem Statement

Despite the growing popularity of digital payment systems in Pakistan, issues such as cybercrime, data breaches, online fraud, privacy risks, and unauthorized access can create uncertainty and discourage consumers from fully relying on digital payment services. Although banks and fintech companies continue to introduce more advanced and convenient digital solutions, some users remain hesitant because they are unsure whether these platforms can adequately protect their financial and personal information.

These concerns are particularly relevant for Generation Z. Although this generation is highly familiar with technology and frequently uses digital platforms, its members are also increasingly aware of privacy and online security risks. As a result, technological familiarity alone may not be sufficient to encourage the continued use of digital payment services. Consumers also need to feel confident about the security of these platforms and trust the institutions providing them.

Previous studies have extensively examined digital payment adoption from the perspectives of technology acceptance, perceived usefulness, ease of use, and service quality. Addressing this gap, how Cybersecurity Assurance and Institutional Trust influence Digital Payment Usage, is important for understanding whether stronger perceptions of cybersecurity and greater trust in financial institutions can reduce consumers' skepticism toward digital financial services. Therefore, this study examines the role of Cybersecurity Assurance and Institutional Trust in encouraging the transition from skepticism toward greater adoption and use of digital payment services among Generation Z consumers in Pakistan.

Study Objectives

1. To investigate the linkage among cybersecurity assurance and digital payment usage for Pakistani Generation Z.
2. To assess the role of trust for digital payment usage and cybersecurity assurance.

Literature Review

Innovation in financial technologies has allowed consumers to perform financial transactions using a variety of methods other than cash, checks, and cards. These advances have speeded up and simplified various financial transactions. These innovative financial systems provide more convenient and efficient ways to perform financial transactions. Early research on the adoption of digital payments focused on the convenience and the usefulness of the technology. The Technology Acceptance Model (TAM) posits that an individual's beliefs and attitudes toward technology affect their intention and behavior toward using the technology. Perceived ease of use and perceived usefulness are the two primary determinants of intention and behavior, and therefore, are the focal points of many studies that use TAM. Financial technology creates a higher level of risk for users compared to other technologies, and thus trust is of utmost importance. Financial technologies and

other traditional technologies differ in regard to the level of importance trust plays in adoption. Traditionally, security and privacy concerns shaped the consumer acceptance of financial technologies, but a growing awareness and concern for data protection and security prompt people to question the security and privacy of various digital platforms.

Further evidence of the role of trust in digital finance is seen in Trust Transfer Theory. Yu et al. (2018) indicate that for consumers, digital trust is built on the relationships they have with financial institutions. Because of this trust, consumers tend to use their mobile payment services and banking apps. A reputation for transparency and reliability, coupled with the perceived ability to protect consumers, provide the foundation for trust in digital finance. As referred to before, the main barrier for entry into digital finance for customers is perceived risk. El Haddad and Aïmeur (2018) showed that consumers have anxiety when they transmit sensitive financial information online, and, because of fears related to hacking, identity theft and loss, and the misuse of their personal information, they feel threatened when using digital financial services. Therefore, there is a need for trust providers to alleviate these fears to ensure clients turn to digital finance.

In Pakistan, the need for security is obvious. Quayyum et al. (2018) show that consumers are cautious about the security of their transactions and payment protection when considering online purchases. If confidence in online payment security and protection is increased, digital transactions will also increase. In Pakistan's case, constant improvements in the legal and regulatory Framework governing the Internet may act to allay consumers' concerns and improve their trust in digital financial services.

Structural assurance plays a role in the formation of trust. Shao et al. (2019) mentioned that digital consumers are more willing to trust a platform when they believe that the platform has sufficient technical and legal systems in place to manage operational risks. Vijayan et al. (2020) also noted the rapid adoption of digital technology has changed users' financial behavior, while at the same time increasing new forms of cybersecurity risks. Given-Wilson et al. (2020) underscored that consumers can't see how digital systems protect and process their information. Therefore, in the absence of direct observation, consumers have to rely on their sense of cybersecurity and trust the reliability of technology and the institution in the digital economy.

This is even more true for Generation Z. Szumski (2020) mentioned that this group of consumers has high awareness of the protection of their personal data and may have concerns about how their data is collected, stored, shared, and used. Though many members of Gen Z are extremely technology-savvy and integrate digital technology in almost all aspects of their daily life, they may still maintain a high level of mistrust towards digital financial services.

Some institutional practices can alleviate these issues. Poerjoto et al. (2021) named positive user experiences, effective customer support, refund mechanisms, secure transactions, and efficient complaint handling as important elements of institutional trust. In developing economies, institutional mechanisms assume greater importance in shaping consumer trust and confidence in digital finance. Consumers are likely to trust a payment platform if they perceive it as a regulated and transparent entity with the capability to respond and address user complaints.

The type and level of assurance also influence the degree of trust in the service. Ahmed et al. (2022) also emphasized encryption as a cybersecurity mechanism to protect financial data. In their study, presence of robust encryption along with assurances of a secure and reliable payment infrastructure positively impacted consumers' trust and confidence in financial transactions. Kumar et al. (2023) also found that negative perception of risk has a limiting effect on the use of digital payments by young consumers in South Asia. However, in the presence of assurances, consumer trust and confidence increased in response to a positive perception of risk.

Khan et al. (2023) also found that perceived assurances of cybersecurity (i.e. encryption, firewalls, and payment gateways) strengthened consumers' trust and confidence in using digital payment platforms. Visible mechanisms make consumers feel safer, which in turn lessens perceived risk. Navalgund et al. (2023) also found similar attitudes among Gen Z in South Asia, where consumers are wary of digital payment systems.

Pakistan-based research has incorporated the domains of security and trust into the traditional dimensions of technology acceptance and behavioral models. Zhang et al. (2023) integrated the aspects of data security and customer trust into the Technology Acceptance Model (TAM) and studied the role of cybersecurity assurance in the context of digital payments among Pakistani banking customers. They found that, indeed, in the presence of trust, the importance of security of the system is reinforced. Trust and confidence in the system to protect the customer's interest assumes more significance than ease and convenience of use in the context of electronic payment systems.

Rani (2023) focused on the integration of artificial intelligence (e.g., to detect and stop suspicious financial transactions) and the implementation of real-time monitoring as technologies to build assurance among customers. The use of AI to build confidence among customers in electronic payment systems is also evident in the studies of Li et al. (2023) and Ahmed et al. (2024).

The recent studies focus on the integration of the aspects of technological security and institutional reputation. Ahmed et al. (2024) found that the reputation of an institution plays an important role in customers' perception of the payment systems of emerging economies. Trust in an institution is reinforced when combined with a positive reputation. In the case of Pakistan, trust and confidence in the payment systems are fortified when combined with the reputation and positive image of the regulating authority (e.g., the State Bank of Pakistan). Stronger and more transparent laws and effective monitoring would build customers' confidence in the payment systems (e.g., the Securities and Exchange Commission of Pakistan).

Further, Zhao et al. (2024) confirmed that trust in institutions can act as a mediator between cybersecurity assurance and the adoption of digital payments. It can be said that users may be willing to take certain digital financial risks if they believe that the institutions are trustworthy and dependable. Hussain et al. (2024) highlighted client-focused security practices as transparency, active fraud management, and service responsiveness and ethical behavior. Schrank (2024) outlined the psychological barriers of the group as anxiety related to technology, privacy and perceived cyber risks. Thus, perceived usefulness may not always be the primary driver in behavior.

Pakistan has made notable progress in strengthening its digital financial system through various institutional and regulatory initiatives. According to the State Bank of Pakistan (2024), the initiatives; National Financial Inclusion Strategy, Raast Instant Payment System, Regulatory Sandbox and digital banking frameworks, are designed to make digital transactions safer, more accessible, affordable, and faster for consumers. At the same time, they support wider financial inclusion and encourage greater documentation of financial activities within the economy.

Ali et al. (2025) discussed the barriers and facilitators of the adoption of digital financial services in the case of emerging markets. Services such as JazzCash and Easypaisa enable customers to perform everyday financial transactions through their smartphones, and are therefore called “financial services operators”. Usage, however, is hindered by barriers such as a lack of confidence and trust, as well as cyber anxiety. Cybersecurity and the support of financial institutions and government agencies help build trust. Nazir et al. (2025) highlighted the use of visible signals of protection as providing assurance in cybersecurity. Riaz et al. (2025) and Shah Fahad (2025) focused on the restoration of trust, and maintained that cybersecurity incidents can lead to an improvement in digital literacy. Trust can also be restored if financial institutions act promptly, clearly, and truthfully, as is particularly valued by the youth. Consequently, Mehmood (2025) concluded that the digital financial services landscape in Pakistan is beyond a ‘first-mover’ competitive edge, and is more focused on the acceptance of the services based on reassuring consumers of security and integrity.

Over time, literature clearly reflects how focus has evolved from the technology itself, to cybersecurity and privacy, to building institutional trust and developing psychological confidence. Generation Z is especially relevant here, because although the members of this generation are heavily involved in the digital space, they are aware of the risks associated with it. While Pakistan’s FinTech market is growing, the concerns of cybersecurity and privacy, coupled with fears of fraud and untrustworthy institutions, mean that a lot of people remain financially exclusive. Literature suggests that in order to overcome digital financial skepticism and encourage adoption of digital payments, combined assurance of both cybersecurity and trust of institutions is a must. While a lot of work focuses on this combined assurance in other contexts, the literature review reveals no works focusing on combined assurance among Gen Z of Pakistan. Therefore, this represents an important area of research.

Methodology

A theoretical framework helps integrate a given study with existing knowledge and describes the relationships among variables. This study synthesizes TAM, TPB and Perceived Risk Theory to examine Digital Payment Usage by consumers of Generation Z in Pakistan.

As proposed by Davis (1989), perceived usefulness and perceived ease of use mainly determine the adoption of technology. This study posits that efforts to improve Cybersecurity Assurance and related Institutional Trust can reinforce user’s confidence in the reliability and usefulness of Digital Payment Systems and increase the perception of security in the Cyber space, thus leading to higher usage of Digital Payments. TPB further states that attitude and subjective norms combined with

perceived behavioral control influence a person's intention toward a behavior (Ajzen, 1991). It is therefore, posited that by addressing the concerns of fraud and breaches of customers' data as well as enhancing customers' trust in the Institution, attitude toward digital payment and intention to use will likely improve.

According to Bauer (1960), uncertainty of negative outcomes and risks influence consumers' behavior. Both trust in the Institution and strong Cybersecurity practices diminish the consumer's perceived risks and increase perceived benefits which in turn, influence consumers' Digital Payment Usage.

Conceptual Framework

A conceptual framework is a diagram, plan, or model of a study, explaining the important elements, and the presumed relationships among them. In this sense, it is a 'plane' of integrated concepts, or a network, that explain a phenomenon or phenomena (Jabareen 2009). It serves as a base for a researcher's theory to explain what will be studied, why it is important, and the nature of the relationships among the variables of the study.

The perceived benefits of FinTech include economic advantages, simplicity, ease of use, and greater transparency. At the same time, users may associate FinTech services with certain risks, particularly financial, cybersecurity, and legal risks. The proposed model examines how each of these perceived benefits and risks influences an individual's intention to use FinTech services. By considering these factors separately, the study seeks to identify which benefits are more likely to encourage individuals to use FinTech and which risks may create hesitation or discourage its adoption. This will provide a better understanding of how users evaluate the advantages and potential concerns associated with FinTech when deciding whether to use such services.

Theoretical Framework and Measurement Constructs

The theoretical framework explores the relationship between cybersecurity, trust, and the adoption of digital payment systems. The framework has two independent variables (Cybersecurity Assurance and Institutional Trust) and one dependent variable (Digital Payment Usage). Cybersecurity Assurance looks at the perception of consumers regarding the encryption, authentication, and privacy protection as well as prevention of fraud and other malicious activities. Institutional Trust looks at the perception of consumers regarding the integrity, competence, and reputation, as well as compliance and responsibility of financial institutions. Digital Payment Usage looks at the intention, preference, and recommendation of consumers for the use of digital payment systems. The framework looks at the digital payment behavior of members of Generation Z in Pakistan.

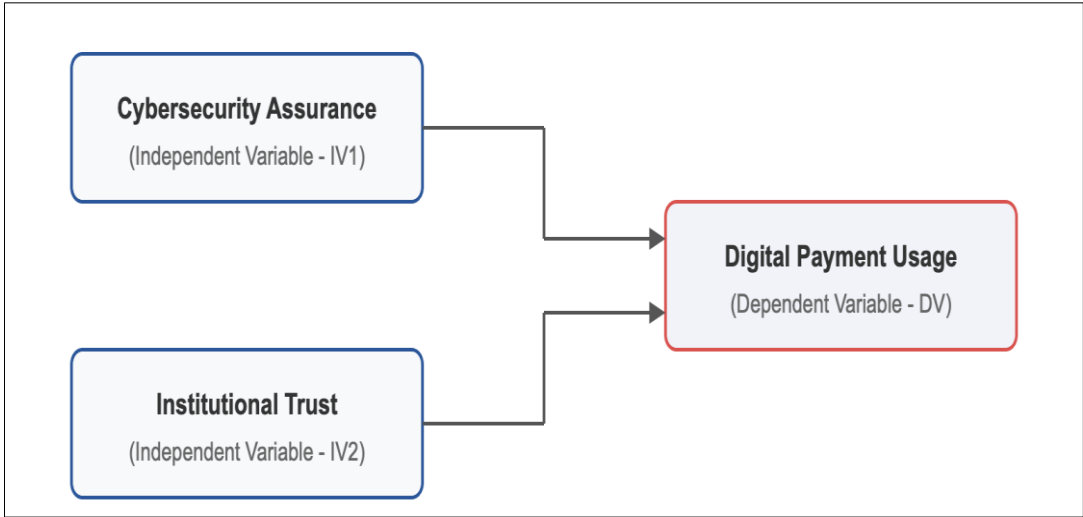


Figure 1 Conceptual Framework

Table 1 Measurement Constructs, Items and Sources

Construct	Items	Measurement Focus	Sources
Cybersecurity Assurance (IV1)	CA1–CA8	Encryption, multi-factor authentication, prevention of unauthorized access, data protection, threat transparency, fraud detection, transaction security, and privacy protection	Zhang et al. (2023); Nazir et al. (2025); Mehrband et al. (2020); Shah Fahad (2025); Riaz et al. (2025); Zhao et al. (2024)
Institutional Trust (IV2)	IU1–IU8	Institutional integrity, SBP monitoring, legal protection, reputation, responsibility, data confidentiality, technical competence, and regulatory compliance	Zhao et al. (2024); Rana et al. (2023); Asghar & Adnan (2024); Iqbal et al. (2022); Hussain et al. (2024); Shah Fahad (2025); Riaz et al. (2025)
Digital Payment Usage (DV)	DU1–DU8	Future usage intention, preference over cash, recommendation, efficiency, Raast usage, daily usage, financial habits, and routine adoption	Li et al. (2023); Ali et al. (2025); Zhao et al. (2024); Zhang et al. (2023); Asif et al. (2025)

Research Hypotheses

H1: A higher level of Cybersecurity Assurance is positively associated with greater Digital Payment Usage.

H2: Greater Institutional Trust is positively associated with increased Digital Payment Usage.

Research Design

Research design provides a clear framework for how data are collected and analyzed to address the research questions and achieve the objectives of a study (Bryman, 2016). In this research, a cross-sectional design was adopted, allowing data to be gathered from respondents at a specific point in time. This design was considered suitable because it enabled the researcher to examine the relationships among the study variables within the selected population. A quantitative research approach was used to provide empirical evidence regarding the relationships between Cybersecurity Assurance, Institutional Trust, and Digital Payment Usage. Data were gathered through a structured questionnaire administered to individuals who had experience using digital payment or FinTech services. This ensured that respondents were familiar with the services being investigated and could provide relevant information based on their actual experiences.

Nature of the Research

This study is quantitative and tests its hypotheses by analyzing numerical data. Research responses were collected online via a structured questionnaire. Internet data collection provided the ability to reach a large number of participants regardless of geographic and time constraints. Quantitative research is appropriate and effective to analyze relationships between variables through the use of available statistical procedures (Babbie, 2020). The use of quantitative research procedures to analyze and test the hypotheses, made it possible to fulfill the requirement of objectivity that is required for higher academic degrees.

Sample Selection and Sampling Technique

A large enough sample is essential for making statistically reliable conclusions and reducing sampling error (Taherdoost, 2017). The sample size was computed using Cochran's (1977) formula for large or unknown population, and 301 respondents was established as the minimum sample requirement. A total of 353 responses were obtained and as such the sample size was within the desired range.

Purposive sampling, a non-probability sampling method, was employed for this study (Etikan et al., 2016). Here, participants were selected based on predetermined conditions that are relevant to the study objectives. The participants for this study were students and working professionals who have knowledge or have used digital payment applications and FinTech services. Purposive sampling was considered appropriate because the study aimed at obtaining respondents who had the knowledge and experience of digital financial services (Tongco, 2007).

Selection of the Study Area

Most of the study participants were from Punjab, Pakistan, with the majority from Faisalabad. Faisalabad was important for the study for several reasons. First, it is an important urban and industrial center. Second, it is rapidly developing digitally and has increasing awareness and availability of digital financial services. Finally, it improved access to the target population and assisted in the primary data collection from the population that is familiar with digital financial services.

Data Collection Method

Data was collected using a structured questionnaire. It was designed based on reviewed literature. The questionnaire had four sections, i.e., demographic information, Cybersecurity Assurance, Institutional Trust, and Digital Payment Usage. It was designed in Google Forms and shared using email and different messaging applications.

The items under constructs were measured using a five-point Likert scale, from 1 = Strongly Disagree to 5 = Strongly Agree. A five-point Likert scale was used because of its simplicity and preference in the survey research (Allen & Seaman, 2007).

Data Preparation Procedure

Data preparation involved editing, coding and cleaning to make data sets complete, accurate and consistent (Hair Jr. et al., 2010; Malhotra, 2020). Editing involved checking responses for errors such as, omissions, inconsistencies, and incompleteness. Coding changed responses from qualitative to quantitative format for data analysis. Excel was used to make the dataset ready for analysis. Data cleaning involved identifying and removing errors such as, duplicates, null values, formatting errors, and invalid responses. Following the aforementioned data preparation procedures, the finalized dataset was ready for analysis.

Data Analysis

Scale Measurement and Reliability Analysis

This study used Cronbach's alpha to assess the internal consistency of measurement items. The rule of thumb for Cronbach's alpha is that values of 0.70 or more indicate acceptable reliability. Composite Reliability (CR) was assessed because, unlike Cronbach's alpha, it accounts for the actual factor loadings of individual items. It was therefore expected that, at a minimum, CR would be comparable to Cronbach's alpha. It was found that a CR of 0.70 or more reflects acceptable reliability.

PLS-SEM

PLS-SEM was used to evaluate the research model. PLS-SEM is a statistical method based on variance and is used to evaluate relations among constructs. It is useful in predictive research where strict normality is not required (Hair et al., 2011).

In PLS-SEM, the measurement model refers to the relationships among the different indicators of each construct, whereas the structural model refers to the relationships among Cybersecurity Assurance, Institutional Trust, and Digital Payment Usage.

Results and Discussion

This section provides analysis and interpretation of the study findings. It starts with demographic characteristics of respondents, followed by descriptive statistics. This is followed by frequency distributions for Cybersecurity Assurance, Institutional Trust, and Digital Payment Usage. The measurement and structural models are evaluated by inner model collinearity, outer loadings, coefficient of determination (R^2), effect sizes (f^2), reliability, convergent and discriminant validity, model fit, path coefficients and hypothesis testing.

Demographical and Categorical Variables

Demographic characteristics provide important contextual information about respondents and facilitate understanding of the sample composition (Bryman, 2016).

Table 2 : Demographic and Categorical Variables

Category	Classification	Percentage (%)
Gender	Female	50.96
	Male	49.04
Age	14–21 years	33.65
	22–29 years	66.35
Education	Matric	4.81
	Intermediate	13.46
	Bachelor's	61.54
	Master's	20.19
Employment	Student	58.65
	Employed	30.77
	Self-employed	5.77
	Unemployed	4.81
Primary Digital Payment App	Jazz Cash	41.35
	Bank Mobile Wallet	26.92
	Easy paisa	15.38
	NayaPay/SadaPay	7.69

Usage Frequency	Raast	3.85
	Do not use	4.81
	Daily	15.38
	2-3 times/week	55.77
	Once/week	10.58
	Rarely	17.31
	Missing/No Response	0.96

The sample was almost equally distributed by gender, with females representing 50.96% and males 49.04%. The majority (66.35%) of respondents were in the age bracket 22-29 years, and 33.65% were in the age bracket 14-21 years. The largest group by education (61.54%) was the Bachelor's, followed by the Master's (20.19%), Intermediate (13.46%), and Matric (4.81%) levels. Students were 58.65% of the respondents, while employed individuals were 30.77% of the respondents.

JazzCash was the most reported (41.35%) payment application, followed by bank mobile wallets (HBL, UBL and Meezan) (26.92%), and Easypaisa (15.38%). Of the respondents, 55.77% used digital payments 2-3 times a week, while 15.38% of respondents used digital payments on a daily basis. Respondents in the study showed awareness and access to digital payments.

Descriptive Statistics

Mean values for CA1-CA7 ranged from 4.000 to 4.272 with CA2 having the highest mean at 4.272, and CA4 having the lowest mean at 4.000. For Digital Payment Usage (DPU1-DPU8), means ranged from 4.109 to 4.218, and DPU3 and DPU8 had the highest means at 4.218. Means for IT1-IT8 ranged from 4.030 to 4.230, and IT1 had the highest mean at 4.230 and IT3 had the lowest mean at 4.030.

The reported median of all indicators was 4.000 showing that the majority of respondents agreed with the statements. Standard deviations for all indicators were approximately between 0.651 and 0.886, indicating moderate level of dispersion. All indicators had negative skewness, indicating that the respondents clustered toward the higher end of the Likert scale. In general, respondents had a positive outlook regarding Cybersecurity Assurance, Institutional Trust, and Digital Payment Usage.

Frequency Distribution

Cybersecurity Assurance

The responses to the cyber assurance items were mostly positive. Regarding CA1, 57.3% agreed and 31.1% strongly agreed with the statement 'high-level encryption protects payment data'. For CA2, 50.5% agreed and 39.8% strongly agreed on multi-factor authentication and OTP. For CA3, 50.5% agreed and 31.1% strongly agreed with the protection of the infrastructure against unauthorized access. CA4, 49.0% agreed and 28.4% strongly agreed on the protection of the data against breaches. The remainder of the items were positive regarding transparency about cyber threats, fraud detection and prevention, and high value transactions, as well as, digital privacy. Item CA8

was positive regarding the protection of the respondents' digital footprint, with 54% agreeing and 35% strongly agreeing. It can be noted that most of the respondents were positive about protection via encryption, authentication, and fraud protection, as well as, privacy and security of high value transactions.

Institutional Trust

Institutional trust also showed positive trends. For IT1, 54% agreed and 35% strongly agreed that service providers act with integrity. For IT2, 51.5% agreed and 31.7% strongly agreed that the State Bank of Pakistan effectively monitors digital payment platforms. IT3, legal protection, received 42.6% agreement and 33.7% strongly agreed. It showed relative uncertainty.

Regarding institutional reputation, IT4, 51.5% agreed and 32.7% strongly agreed, while IT5, responsibility for technical errors, received 44.6% agreement and 35.6% strongly agreed. Respondents showed confidence in service providers and technical teams, as well as in institutional security policies and practices. Confidence in the service providers' ability to align with users' expectations and adapt to their needs, showed an 85.5% agreement and 40% strongly agreed. Respondents showed 77.5% agreement and 34.7% strongly agreed in confidence that service providers would be able to meet the needs of stakeholders.

Digital Payment Usage

Responses to Digital Payment Questions also show strong tendencies. 53.5% agreed and 30.7% strongly agreed they would use digital payments in the future, based on DPU1. DPU2 showed 51.5% agreed and 33.7% strongly agreed they prefer mobile wallets over cash. Finally, 53.5% agreed and 34.7% strongly agreed they would recommend the use of digital payment applications to others, based on DPU3.

Also, 85.2% of the respondents felt digitized payments were better than cash (DPU4). Answers to DPU5 (which focused on Raast's instant money transfer service) showed an 85% positive response. DPU6 showed an 84% positive response to using digital payment services on a daily basis, and respondents felt improved financial habits due to using digital payment services (DPU7) at a rate of 87.2%. DPU8 recorded an 89.1% positive response to incorporation of digital payment services in respondents' day-to-day activities. The findings indicated that participants were repeatedly using digital payment services.

Inner Model Collinearity

Variance Inflation Factor (VIF) was used to examine potential multicollinearity between Cybersecurity Assurance and Institutional Trust.

Table 3: Inner Model Collinearity

Predictor Relationship	VIF Value
CA predicting DPU	4.323
ITI predicting DPU	4.323

Both VIF values are below the 5.00 threshold used in the study, indicating no severe multicollinearity. Although both exceed the more conservative criterion of 3.3, the study’s adopted threshold supports proceeding with structural model assessment.

Outer Loadings

Outer loadings assess indicator reliability, with values around 0.708 or higher generally considered satisfactory.

Table 4: Outer Loadings

Construct	Indicator Loading Range
Cybersecurity Assurance	0.823–0.912
Digital Payment Usage	0.771–0.930
Institutional Trust	0.829–0.953

For Cybersecurity Assurance, loadings ranged from CA2 = 0.823 to CA4 = 0.912. Digital Payment Usage ranged from DPU6 = 0.771 to DPU2 = 0.930. Institutional Trust ranged from IT5 = 0.829 to IT7 = 0.953. All reported indicators therefore exceeded the recommended threshold and were retained in the measurement model.

R² Value

The coefficient of determination measures the proportion of variance in the dependent variable explained by its predictors.

Table 5: R² Value

Variable	R²	Adjusted R²
DPU	0.732	0.727

Cybersecurity Assurance and Institutional Trust jointly explain 73.2% of the variance in Digital Payment Usage, while 26.8% remains attributable to factors outside the model. The adjusted R² of 0.727 demonstrates that explanatory power remains stable after adjustment. Based on the criteria of 0.75, 0.50, and 0.25 for substantial, moderate, and weak explanatory power respectively, the obtained R² is close to the substantial level.

F-Square Values

Effect size (f^2) measures each predictor’s individual contribution to the endogenous construct.

Table: 6 F^2 Value

Predictor and Outcome	Effect Size (f^2)	Magnitude of Effect
CA predicting DPU	0.208	Moderate
ITI predicting DPU	0.133	Small

Using thresholds of 0.02, 0.15, and 0.35 for small, medium, and large effects, Cybersecurity Assurance demonstrates a medium effect (0.208), whereas Institutional Trust demonstrates a small effect (0.133). Thus, Cybersecurity Assurance contributes more strongly to the explained variance in Digital Payment Usage.

Reliability and Convergent Validity

Table 7: Reliability and Convergent Validity

Study Construct	Alpha (α)	Reliability	Reliability (ρ_A)	Composite Reliability (ρ_C)	Average Variance Extracted (AVE)
CA	0.948		0.950	0.958	0.764
DPU	0.963		0.964	0.969	0.797
ITI	0.964		0.970	0.970	0.800

All Cronbach’s Alpha, ρ_A , and Composite Reliability values exceed 0.70, demonstrating strong internal consistency. Similarly, all AVE values exceed 0.50, supporting convergent validity. Therefore, the measurement model demonstrates satisfactory reliability and convergence.

Discriminant Validity

HTMT was used to assess discriminant validity.

Table 8: Discriminant Validity

Construct Pair	HTMT Ratio
CA ↔ DPU	0.871
ITI ↔ DPU	0.847
CA ↔ ITI	0.914

The values 0.871 and 0.847 are less than 0.90. The Cybersecurity Assurance–Institutional Trust HTMT, however, is 0.914, which is greater than 0.90. The study states the 95% bias-corrected and

accelerated confidence interval did not include 1.00, so these constructs are treated as empirically distinguishable.

Cross-loading analysis also showed every indicator loaded more strongly to its corresponding construct than to other constructs. For example, CA4 loaded to Cybersecurity Assurance by 0.912, DPU2 loaded to Digital Payment Usage by 0.930, and IT7 loaded to Institutional Trust by 0.953. Therefore, indicator-level discriminant validity was considered satisfactory.

Estimated Model Fit

Table 9 : Estimated Model Fit

Model Fit Measure	Saturated Value	Model Estimated Value	Model
Standardized Root Mean Square Residual (SRMR)	0.058	0.058	
Squared Euclidean Distance (d_ ULS)	0.938	0.938	
Geodesic Distance (d_ G)	2.010	2.010	
Chi-Square (χ^2)	888.201	888.201	
Normed Fit Index (NFI)	0.754	0.754	

With a SRMR of 0.058, the model fits within the accepted range of 0.08. D_ ULS is 0.938. The model also shows D_ G of 2.010 and Chi-square of 888.201. The NFI is 0.754, which, with the benchmark of 0.90, also indicates that the model should be interpreted with caution. Considering the SRMR, the model was considered to be adequately appropriate for further structural analysis.

Path Coefficients

Table 10 : Path Coefficients

Predictor–Outcome Relationship	Standardized Path Coefficient (β)
CA predicting DPU	0.491
ITI predicting DPU	0.392

We found Cybersecurity Assurance to have a positive coefficient of $\beta = 0.491$, indicating a higher level of Digital Payment Usage when the perception of Digital Security is stronger. A similar positive relationship with Digital Payment Usage was found for Institutional Trust ($\beta = 0.392$). Based on the coefficient estimates, Cybersecurity Assurance is expected to show a relatively stronger relationship in the model.

Table 11: Hypothesis Testing

Hypothesis	Structural Path	β	f^2	Result
H1	CA $\rightarrow$ DPU	0.491	0.208	Supported
H2	ITI $\rightarrow$ DPU	0.392	0.133	Supported

H1: Cybersecurity Assurance positively and significantly influences Digital Payment Usage. Results indicate $\beta = 0.491$ and $f^2 = 0.208$, and H1 is supported. The result indicates that respondents who believe that their personal and financial information is protected, increases digital payment usage.

H2: Positive and significant influence of Institutional Trust on Digital Payment Usage. The results indicate $\beta = 0.392$ and $f^2 = 0.133$, and H2 is supported. The result suggests that respondents who believe banks and financial institutions serve their best interest, increase the usage of Digital Payments.

The model explains 73.2% of the variation in Digital Payment Usage ($R^2 = 0.732$). Cybersecurity Assurance presents the larger path coefficient (0.491) and medium effect size (0.208), and Institutional Trust presents a positive coefficient (0.392) and small effect size (0.133). Therefore, findings support the research model and suggest that both Cybersecurity Assurance and Trust of Financial Institutions impact Digital Payment Usage of Generation Z of Pakistan.

It is important to note that the hypothesis table supplied in the source indicates both hypotheses as “Supported”, but the displayed table does not report t-values or p-values. Thus, no additional claim regarding hypothesis testing can be asserted, unless the corresponding SmartPLS bootstrapping results are available.

Conclusion

This study assesses Cybersecurity Assurance and Institutional Trust and its impact on Digital Payment usage within Generation Z in Pakistan. Recent trends in the rise of digital financial services coupled with existing challenges in the trust and reliability of service providers, concerns in privacy and cybersecurity and the lack of regulations have prompted the need for this study. A Quantitative research design was adopted. Data was collected via a structured questionnaire with a Likert scale of 5. Purposive sampling was utilized to obtain participants knowledgeable in FinTech, Digital Payment systems and associated risks. The sample size was 301, and the data mainly originated from Punjab and Faisalabad. Data was analyzed through PLS-SEM using SmartPLS 4.

The measurement model indicated acceptable levels of reliability and validity. Cronbach’s Alpha was 0.948 for Cybersecurity Assurance, 0.963 for Digital Payment Usage and 0.964 for Institutional Trust, suggesting strong levels of internal consistency. In addition, AVE was 0.764, 0.797 and 0.800 respectively, suggesting convergent validity. The HTMT value between Cybersecurity Assurance and Institutional Trust was 0.914. The 95% bias-corrected and accelerated confidence interval did

not include 1.00, and cross-loadings supported that all the indicators loaded on their respective constructs.

The structural model demonstrated substantial explanatory power with a R^2 of 0.732 and an adjusted R^2 of 0.727 for Digital Payment Usage. Cybersecurity Assurance and Institutional Trust together accounted for 73.2% of the variance in Digital Payment Usage with the remaining 26.8% being explained by factors outside the model. Cybersecurity Assurance had an effect size of $f^2 = 0.208$ and Institutional Trust had an effect size of $f^2 = 0.133$.

Positive relationships were estimated for both constructs. The path coefficient for Cybersecurity Assurance was $\beta = 0.491$ and the path coefficient for Institutional Trust was $\beta = 0.392$. The hypothesis testing also confirmed support for both H1 and H2. Cybersecurity Assurance also had the larger effect size and path coefficient for the estimated model.

The findings show that the use of digital payments by respondents is due to the presence of digital technology and the confidence of respondents in the security of digital transactions and the financial system. Respondents that have confidence in the safety of their financial and personal information and trust the financial system and service providers report increased use of digital payment services.

Recommendations

The study provides recommendations related to improving the cybersecurity of digital payment service providers and banks and financial institutions.

Digital payment service providers should enhance their cybersecurity, including the use of MFA, biometrics, encryption, safe and secure transaction and real-time fraud detection mechanisms. Although technical measures help secure the system, if the end users are not aware of the protective measures, they may be reluctant to use the service. Therefore, along with such measures, the service providers should communicate to the users about the protective measures.

Banks and financial institutions should strengthen institutional trust through transparency, reliability, responsive customer service, and effective complaint and dispute resolution. Users should be given information about transaction security, privacy and fraud protection, and their rights in case of unauthorized transactions. Banks and other financial institutions should work with fintech to enhance secure and user-friendly digital financial services, especially for Gen Z.

For the State Bank of Pakistan, and other similar agencies, policies relating to cybersecurity should be enhanced to include stringent requirements for user authentication and data protection, monitoring of fraud and unauthorized access, as well as other transaction safety measures. Enhancing accountability through regular security audits and the mandatory reporting of security breaches and incidents may also help. Consumer protection mechanisms should be strengthened and improved and transparent complaint resolution and dispute resolution mechanisms should be established.

Future Studies

This study has a number of limitations. First, purposive sampling was used. Therefore, future researchers can increase generalizability by adopting probability sampling and using larger sample sizes. Additional data should also be collected in different regions and provinces of Pakistan since this study was conducted in one province, Punjab, and within that province in one city, Faisalabad.

Second, this study explains 73.2% of the Digital Payment Usage variable, meaning 26.8% of the variance is unexplained. Future researchers can extend the conceptual framework of this study by adding variables such as perceived ease of use, perceived usefulness, social influence, technology anxiety, perceived risk, and other concerns, as well as digital financial literacy.

Third, future researchers can analyze Generation Z and the Millennial and older age groups to assess whether cybersecurity and institutional trust drive the same behavior for different age groups. Comparative studies between Pakistan and other nations with similar or higher levels of economic development can test the same hypothesis with other regions.

Finally, future researchers can employ different research methodologies to test other hypotheses. Longitudinal studies can test whether an individual's digital payment behavior changes with time. Other studies can analyze a single payment system or payment platform. Larger, more comparative and longer studies can test other research hypotheses involving Cybersecurity, Institutional Trust, Digital Financial Inclusion, and Payment Systems.

Reference

- Ahmed, M., Khan, R. and Ali, S. 2022. Role of encryption technology in cybersecurity assurance and digital financial systems. *Journal of Digital Security* 14(2): 115-129.
- Ahmed, S., Rahman, T. and Noor, F. 2024. System quality and institutional trust in emerging digital payment networks. *International Journal of Financial Technology* 11(1): 44-60.
- Ali, H., Raza, M. and Karim, S. 2025. Barriers and facilitators of fintech adoption in emerging economies. *Journal of Financial Innovation* 18(3): 201-220.
- Asghar, M. and Adnan, R. 2024. Cybersecurity regulations and digital financial protection in Pakistan. *Pakistan Journal of Cyber Law* 9(1): 77-92.
- Awan, A., Hussain, M. and Tariq, U. 2019. Cybersecurity legislation and digital financial risks in Pakistan. *Journal of Information Security Studies* 7(2): 88-103.
- Commerce Research 24:3-35. ou H.-S. 2018. What makes users willing or hesitant to use Fintech? the moderating effect of user type. *Industrial Management & Data Systems* 118:541-569.
- Economia 15:243-258. aitama, A. 2019. The mobile payment fintech continuance usage intention in Indonesia. *Jurnal*
- El Haddad, R. and Aïmeur, E. 2018. Toward a model of online payment and privacy fears. *Proceedings of the International Conference on e-Commerce and Security*: 115-123.
- Fortes, N., Rita, P. and Pagani, M. 2017. The effects of privacy concerns in online purchasing behavior. *Journal of Consumer Behaviour* 16(5): 453-462.

- Given-Wilson, Z., McCarthy, S. and Wilson, C. 2020. Human dependence on digital systems and cybersecurity challenges. *Cyber Psychology Review* 12(4): 266-281.
- Hair Jr, J.F., W.C. Black, B.J. Babin and R.E. Anderson. 2010. *Multivariate data analysis, Multivariate data analysis*. p. 785-785.
- Hussain, A., Malik, S. and Rehman, H. 2024. Customer protection practices and institutional trust in digital finance. *Pakistan Journal of Business and Economics* 17(2): 55-71.
- Khan, A., Iqbal, N. & Shah, F. 2023. Cybersecurity infrastructure and consumer confidence in digital payment systems. *Journal of Financial Technology and Security* 10(3): 141-158.
- Kumar, P., Singh, R. and Ahmed, Z. 2023. Perceived risk and trust in digital payment adoption among youth consumers. *Asian Journal of Finance and Banking* 8(2): 90-108.
- Leem, A. 2021. Fintech revolution, perceived risks and Fintech adoption: Evidence from financial industry of pakistan. *International Journal of Multidisciplinary and Current Educational Research* 3:191-205.
- Li, X., Zhao, H. and Wang, L. 2023. Privacy assurance and consumer trust in online financial services. *International Journal of Consumer Studies* 19(3): 200-216.
- Mehmood, S. 2025. Digital financial transformation and consumer trust in Pakistan. *Pakistan Journal of Finance and Banking* 20(1): 31-49.
- Navalgund, R., Sharma, P. and Kiran, V. 2023. Generation Z behavior toward digital payment adoption. *Journal of Consumer Technology* 15(2): 73-89.
- Nazir, M., Abbas, T. and Rauf, A. 2025. Multi-factor authentication and cybersecurity assurance in fintech systems. *International Journal of Cyber Finance* 13(1): 98-116.
- Qayyum, A., Javed, M. and Saleem, R. 2018. Safe payment mechanisms and e-shopping behavior in Pakistan. *Pakistan Journal of Commerce and Social Sciences* 12(3): 601-620.
- Rani, S. 2023. Artificial intelligence and fraud detection in digital payment systems. *Journal of Financial Cybersecurity* 9(4): 177-194.
- Rashid, A., Khan, S., Shah, A., & Ali, S. (2024). Interplay of Green Construction Procurement and Logistic Service Innovation: Advancing Sustainable Economic Growth and Sustainable Development Goals. *International Journal of Social Science & Entrepreneurship*, 4(1), 1-21.
- Rashid, A., Shah, A., Khan, S., Adamjee, M. A., & Shahab, A. (2024). Potential of Cactus Leather in Pakistan's Leather Industry: A Qualitative Analysis. *International Journal of Social Science & Entrepreneurship*, 4(3), 1-16.
- Rashid, A., Shah, A., Ain, H. N. U., & Khan, S. (2024). Impact Of Innovation and Training & Development on Operational Performance: Mediation of Green Lean Six Sigma. *THE ASIAN BULLETIN OF GREEN MANAGEMENT AND CIRCULAR ECONOMY*, 4(2), 4-2.
- Riaz, U., Khalid, M. and Aslam, F. 2025. Cybersecurity awareness and digital payment adoption behavior. *Journal of Digital Banking and Finance* 16(2): 122-139.
- S.K.A., B. Nagvi and F. Tanveer. 2018. Is Pakistan ready to embrace Fintech innovation? 7. Y.S. Yang, S. Xiao and B.I. Park. 2024. What makes consumers trust and adopt fintech? An empirical investigation in China. *Electronic*
- Schrank, T. 2024. Technology anxiety and digital payment adoption among Generation Z consumers. *International Journal of Consumer Psychology* 21(1): 50-68.

- Seed, K., S. Aslam, S. Jabbar, S. Aslam and F. Noreen. 2024. Perceived Trust and Its Antecedents' Impact on Intentions to Use Fintech: Evidence from Pakistan. *Bulletin of Business and Economics (BBE)* 13:573-582.
- Shah Fahad, M. 2025. Trust recovery mechanisms in fintech and digital financial platforms. *Journal of Financial Services Marketing* 14(2): 144-161.
- Shah Fahad, M. 2025. Trust recovery mechanisms in fintech and digital financial platforms. *Journal of Financial Services Marketing* 14(2): 144-161.
- Shao, Z., Zhang, L. and Guo, Y. 2019. Structural assurance and trust in mobile payment services. *Electronic Commerce Research and Applications* 33:100824.
- Shao, Z., Zhang, L. and Guo, Y. 2019. Structural assurance and trust in mobile payment services. *Electronic Commerce Research and Applications* 33:100824.
- Silva, M., H. Perera and P. Kumara. 2023. Effect of perceived risk on behavioural intention of using digital financial services: Exploring the theoretical gap. *South Asian Journal of Business Insights* 3
- Singh, S., M.M. Sahni and R.K. Kovid. 2020. What drives FinTech adoption? A multi-method evaluation using an adapted technology acceptance model. *Management Decision* 58:1675-1697.
- State Bank of Pakistan (SBP). 2022. Digital Bank Regulatory Framework. State Bank of Pakistan, Karachi, Pakistan.
- State Bank of Pakistan (SBP). 2022. Digital Bank Regulatory Framework. State Bank of Pakistan, Karachi, Pakistan.
- Syakinah, F. 2024. Factors Influencing Gen Z's Intention in Adopting Islamic Fintech Payment Digital Services. *JPS (Jurnal Perbankan Syariah)* 5:70-89.
- Taherdoost, H. 2017. Determining sample size; how to calculate survey sample size. *International Journal of Economics and Management Systems* 2
- Tang, K.L., C.K. Ooi and J.B. Chong. 2020. Perceived risk factors affect intention to use FinTech. *Journal of accounting and finance in emerging economies* 6:453-463.
- Venkatesh, V., M.G. Morris, G.B. Davis and F.D. Davis. 2003. User acceptance of information technology: Toward a unified view. *MIS quarterly*:425-478.
- Vijayan, P., Kumar, S. and Thomas, A. 2020. Digital finance and technological transformation in modern economies. *International Journal of Financial Innovation* 5(3):188-205.
- Vučinić, M. and R. Luburić. 2022. Fintech, risk-based thinking and cyber risk. *Journal of Central Banking Theory and Practice* 11:27-53.
- Witha, B., I.T. Hawaldar and N. Kumar. 2022. Continuance intentions to use FinTech peertopeer payments apps in India. *Heliyon* 8
- Yan, H. and Pan, S. 2015. Examining mobile payment user adoption from the perspective of trust transfer. *International Journal of Networking and Virtual Organisations* 15(2/3):136-151.
- Yu, C., Liu, Y. and Huang, J. 2018. Understanding mobile payment users' continuance intention from a trust transfer perspective. *Information Technology and People* 31(2): 456-476.
- Zhang, Y., Ahmed, N. and Khan, S. 2023. Data security, customer trust, and digital banking adoption in Pakistan. *Journal of Islamic Banking and Finance* 40(2): 84-101.

Zhao, L., Chen, H. and Malik, A. 2024. Trust determinant and digital payment adoption behavior. International Journal of Electronic Finance 12(1): 66-83.