

The Impact of Cybersecurity and Digital Fraud Concern on Consumers Adoption of Electronic Payments System In India

Dr. Swapnil Sihare

Research Scholer, Rani Durgavati Vishwavidyalaya (RDVV),
Jabalpur, India (482002)
Email: swapnil.sihare24@gmail.com

ABSTRACT

The adoption of Electronic Payment Systems (EPS) has transformed financial transactions by offering speed, convenience, and accessibility, this rapid digitalization has also increased exposure to cybersecurity threats and digital fraud. Incidents such as phishing, identity theft, malware attacks, and unauthorized transactions pose serious challenges to consumers and financial institutions, ultimately affecting trust and adoption rates. This paper examines the relationship between cybersecurity risks and digital fraud in electronic payment systems, identifies major threat vectors, and evaluates preventive measures including regulatory frameworks, technological solutions, and consumer awareness. The rapid diffusion of Electronic Payment Systems (EPS) in India has transformed consumer payment behaviour, shifting transactions from cash-based to digital platforms such as UPI, NEFT, RTGS, IMPS, AEPS, digital wallets, and Point of Sale (PoS) systems. This transformation has been driven by technological advancement, government initiatives toward a cashless economy, and increased smartphone penetration. However, alongside these benefits, concerns related to cyber security have emerged as a critical determinant of consumer trust and adoption. This study investigates consumer perception, satisfaction, and behavioural intention toward the adoption of Electronic Payment Systems in India, with a specific emphasis on cyber security concerns. Drawing on primary survey data collected from 226 respondents in Jabalpur, Madhya Pradesh, the research examines how usability, service quality, internet banking experience, and perceived security influence consumer satisfaction. The findings indicate that while most users recognize the convenience and societal benefits of digital payments, their continued usage is strongly conditioned by their confidence in cyber security safeguards such as encryption, two-factor authentication, fraud detection mechanisms, and secure digital infrastructure.

KEYWORDS: Electronic Payment Systems, Cybersecurity, Digital Fraud, Online Transactions, Financial Technology

1.1 INTRODUCTION.

1.1.1 INTRODUCTION OF ELECTRONIC PAYMENTS SYSTEM

Electronic Payment Systems, such as Unified Payment Interface (UPI), internet banking (NEFT, RTGS, IMPS), Digital wallets, and Aadhaar Enabled Payment Systems (AEPS), have transformed consumer transactions by enabling cashless, secure, and real-time payments. The increasing reliance on these platforms has been accompanied by challenges regarding user trust, technological literacy, and fraud prevention. The mobile based e-payment wallets, the internet banking, the UPI based e-payment modes, bar codes, point of sale and account to account transactions, plastic money (debit & credit card) and addhar enabled payment system (AEPS) etc.

1.1.2 INTRODUCTION OF CYBER SECURITY

Phishing and social engineering attacks involve deceptive communication designed to trick users into revealing sensitive information such as passwords, PINs, or one-time passwords. These attacks exploit human behaviour rather than technical weaknesses and remain one of the most common causes of digital fraud in electronic payments.

Malware and Hacking Attacks

Malware attacks target users' devices or financial institution systems to gain unauthorized access to transaction data. Trojans, spyware, and keyloggers are frequently used to capture sensitive information, leading to financial losses and data breaches.

Card-Not-Present and Identity Theft Fraud

Card-not-present fraud occurs when stolen card details are used for online transactions without physical verification. Identity theft further exacerbates this problem by allowing fraudsters to impersonate legitimate users and access digital payment accounts.

1.1.3 INTRODUCTION OF DIGITAL FRAUD

Digital Fraud or Cyber Fraud is the unethical activity are performed through the online platforms and digital technology to device people for financial gain, stealing personal data or gaining unauthorized access. The various methods of Digital Fraud are used by the hackers like phishing, malware, spam mail, fake website and unauthorised links.

1.1.3.1 FACTORS CONTRIBUTING TO DIGITAL FRAUD

Technological Complexity

The integration of multiple digital platforms, third-party applications, and open banking APIs increases system complexity and security vulnerabilities. Weak authentication mechanisms and outdated systems further elevate fraud risks.

Lack of Consumer Awareness

Limited digital literacy and lack of awareness regarding cybersecurity practices make consumers vulnerable to fraud. Users often unknowingly share confidential information or fall victim to fraudulent links and applications.

Regulatory and Enforcement Challenges

Although regulatory frameworks exist, inconsistent enforcement and rapidly evolving fraud techniques make it difficult to maintain comprehensive protection against cyber threats.

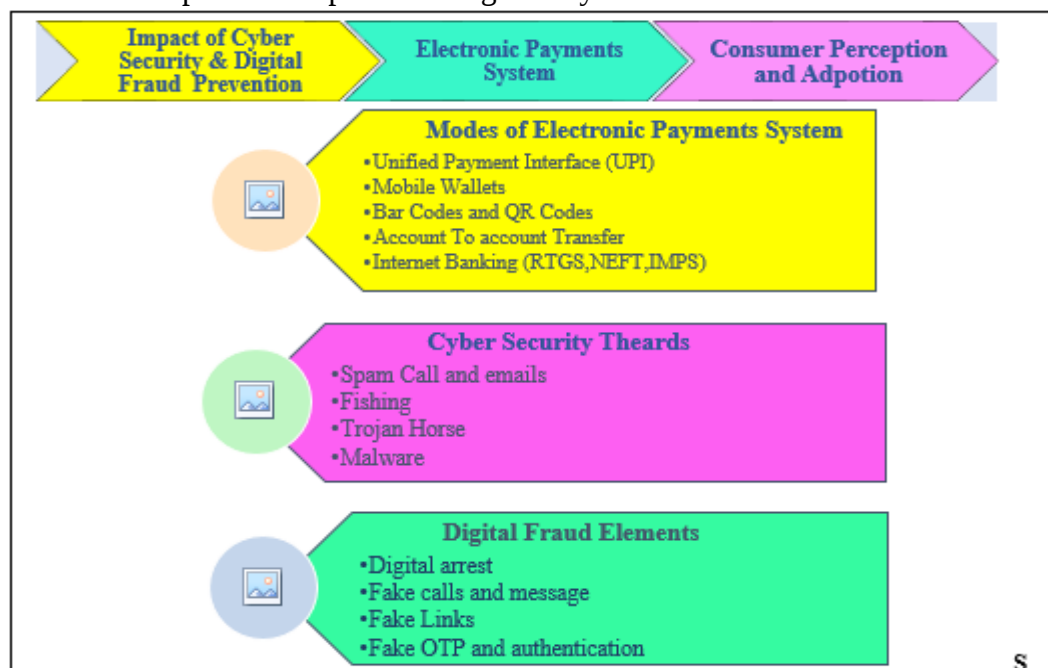
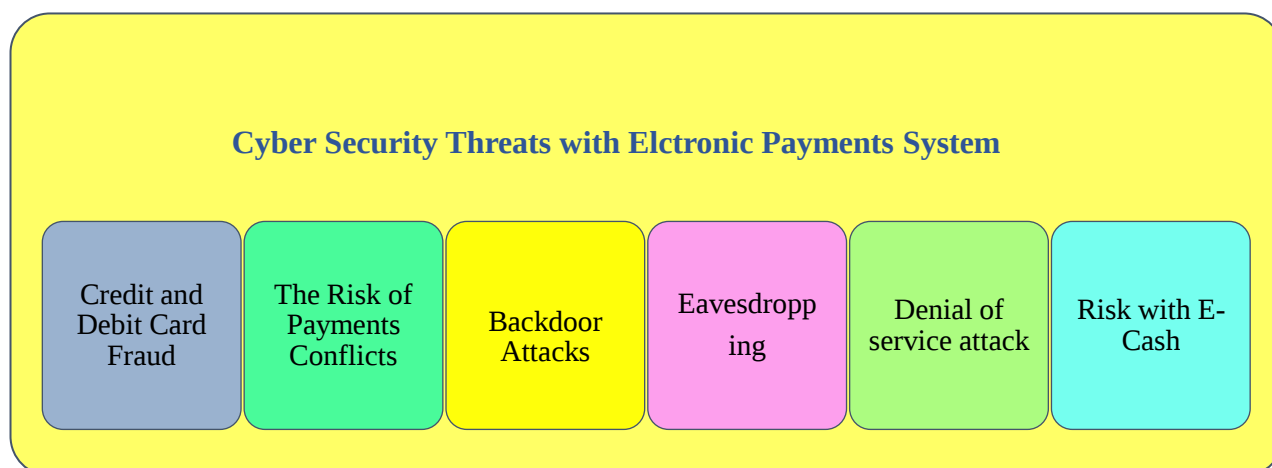


Figure No.1 Impact of Cyber Security & Digital Fraud Concern with Consumer Adoption of Electronic Payments System in India. (Researchers Concept)



1.6 CYBER SECURITY SYSTEM AND ITS THREATS ON ELECTRONIC PAYMENTS SYSTEM

Figure:2 The various Threat with Cyber Security for Adoption of Electronic Payments System (Researcher's Concept)

CHAPTER NO.2

2.1 REVIEW OF LITERATURE

Zhang et al., (2019) has mentioned in their study about the Cyber Security fraud in Digital payments or mobile payments facing various security related frauds like SIM swap, unauthorised transection during the adoption of Digital Payments system like UPI, mobile wallets, Internet Banking transactions are with risk due to Cyber security related threads for users. **Ardiansah et.al (2019)** The Researchers have mentioned the “Consumer Buying Behaviour’ for Electronic Payments System as the purchase intention having a weak association with security during the transaction with Electronic Payments System. Privacy is also an important consideration with using this method to study consumer buying behaviour towards the settlement of electronic transactions in a very safe and secure form. Safety and security are the most common elements engaged in all electronic transactions and evaluate the consumers’ buying behaviour aspects. **Acquisti et al., (2015)** has mentioned in their study that privacy is the big concern when monitoring customer data for fraud detection. The main challenge with the Electronic Payments System is the Cyber Fraud and Cyber Security related threads directly affecting the adoption of Electronic Payments System by the users and the privacy related doubt s are affecting the users mind for decision making for adoption of Electronic Payments System with Cyber security related concern. **Singh et.al (2012)** The Researchers have mentioned in their study the security measurement involved in the Electronic Payments System. The payment via internet or electronic payment methods is such a very important consideration for electronic payments users. Internet network and connectivity of the internet are very important aspects for Electronic Payments users to smarter transactions anytime and anywhere approach. In the current time scenario, Electronic Payments users are mostly adopting mobile wallets for all electronic transactions and E-Commerce marketing with the help of the internet. Mobile phone-based mobile wallets are playing a very important role in E-commerce business activity and also in all digital transactions. **Briggs & Brooks (2011)** The Researchers have described the Electronic Payments System as a form of interconnection between one party and individuals aided by banks or any other financial sector & inter-switch houses that enable all transactions electronically settled by electronic service providers and internet banking service providers with the help of an internet network. All electronic transactions are only possible through internet connectivity. The Electronic Payments System and E-commerce are interdependent with one another and without the Electronic Payments System E-commerce business activity can’t be imagined.

2.2 RESEARCH GAPS

Despite the growing body of literature on electronic payment systems (EPS), several critical gaps remain. **First**, existing studies predominantly adopt a **technology-centric or institutional perspective**, with limited emphasis on **consumer perceptions and behavioural responses** to cybersecurity and digital fraud risks. **Second**, cybersecurity and digital fraud are frequently examined as independent constructs, resulting in a **fragmented understanding** of their combined influence on consumer adoption decisions. **Third**, although

India represents one of the fastest-growing digital payment ecosystems globally, **empirical evidence grounded in the Indian consumer context remains insufficient**, particularly outside metropolitan regions. **Fourth**, the literature inadequately integrates **psychological and perceptual dimensions** such as perceived vulnerability, trust erosion, and risk tolerance within established technology adoption frameworks. Finally, most prior studies focus on **initial adoption intention**, overlooking post-adoption outcomes such as continued usage, avoidance behaviour, and trust recovery following fraud incidents.

CHAPTER NO.3 RESEARCH METHODOLOGY

3.1 RESEARCH DESIGN

Exploratory research is designed to provide a background, to familiarize, and as the word implies, just “explore”, the general subject. A part of exploratory research is the investigation of relationships among variables without knowing why they are studied. Researcher has also adopted the Descriptive Research Design for study about the Consumer Buying Behaviour for Electronic Payments System.

3.2 UNIVERSE POPULATION & SAMPLE AREA

The universe of the study covers PAN India, with Jabalpur, Madhya Pradesh as the primary sample location. Simple random sampling was applied, ensuring equal probability of selection. A total of **226** valid responses were analysed from **282** numbers of total respondents.

Samples were collected from different sample areas of the universe of the population targeted. Sample areas were **Jabalpur** city of **Madhya Pradesh State**, was the population of the study. PAN India is the universe of the study. This study adopts both exploratory and descriptive designs. Exploratory research offers a conceptual understanding, while descriptive analysis issued to assess consumer behaviours.

3.3 RESEARCH OBJECTIVES

1. To assess consumer awareness level with adoption of Electronic Payments System and measure the risks factors enabled with Cyber Security and Digital Fraud.
2. To evaluate the techniques of reduction of risks factors of Cyber Security and growth potential of Electronic Payment Systems in India
3. To examine consumer satisfaction with adoption Electronic Payment Systems with Cyber Security and Digital Fraud preventions techniques.
4. To analyse the role of Cyber Security to shaping the consumer trust for adoption of Electronic Payments System with Digital Fraud identification.

CHAPTER NO.4 DATA COLLECTION, ANALYSIS & INTERPRETATIONS

Primary data was collected via structured questionnaires. Data was analysed using statistical tools to determine relationships between AI features and consumer participation.

PART A

4.1 THE DEMOGRAPHICAL ANALYSIS OF DATA OF AREA, AGE, SEX, EDUCATION, INCOME AND MARITAL STATUS

Table No.1				
Areas	Respondents from Urban Areas	Respondents from Semi Urban Areas	Respondents from Rural Areas	Total Numbers of Respondents
Response	98	77	51	226

Interpretation:

The following Table No.1 of Area of belongings of the respondents and divided into three categories, urban, semi urban and rural areas of belongings of the respondents. Mostly respondent (98) are belongings to the

urban areas in demographical analysis.

Table No.2				
Gender	Male Respondents	Female Respondents	LGBT Respondents	Total Numbers of Respondents
Response	104	97	25	226

Interpretation:

The following Table No.2 of Gender category of the respondents are divided into three categories, Male, Female and LGBT category of the respondents. Mostly respondent (104) are belonging to male category of gender analysis in demographical analysis.

Table No.3				
Education	Higher Educated	Educated	Illiterate	Total numbers of Respondents
Response	83	106	37	226

Interpretation:

The following Table No.3 of education status of the respondents are divided into three categories, highly educated, educated and illiterate respondents. Mostly respondent (106) are belonging into the category of the educated category in demographical analysis.

Table No.4				
Marital Status	Married Respondents	Unmarried Respondents	Others Respondents	Total numbers of Respondents
Response	100	79	46	226

Interpretation:

The following Table No.4 of Marital Status of the respondents are divided into three categories, Married, Unmarried and others respondents. Mostly respondents (100) are belonging into the category of the Married group in demographical analysis.

Table No.5				
Age Group	Age Between (In Years) 15-30	Age Between (In Years) 31-45	Age Between (In Years) 46-60	Total numbers of Respondents
Response	56	102	68	226

Interpretation:

The following Table No.5 of age group of the respondents are divided into three categories, 15-30, 31-45 and 46-60 years of age. Mostly respondent (102) are belonging into the category of the age group of 31-45 years of age group in demographical analysis.

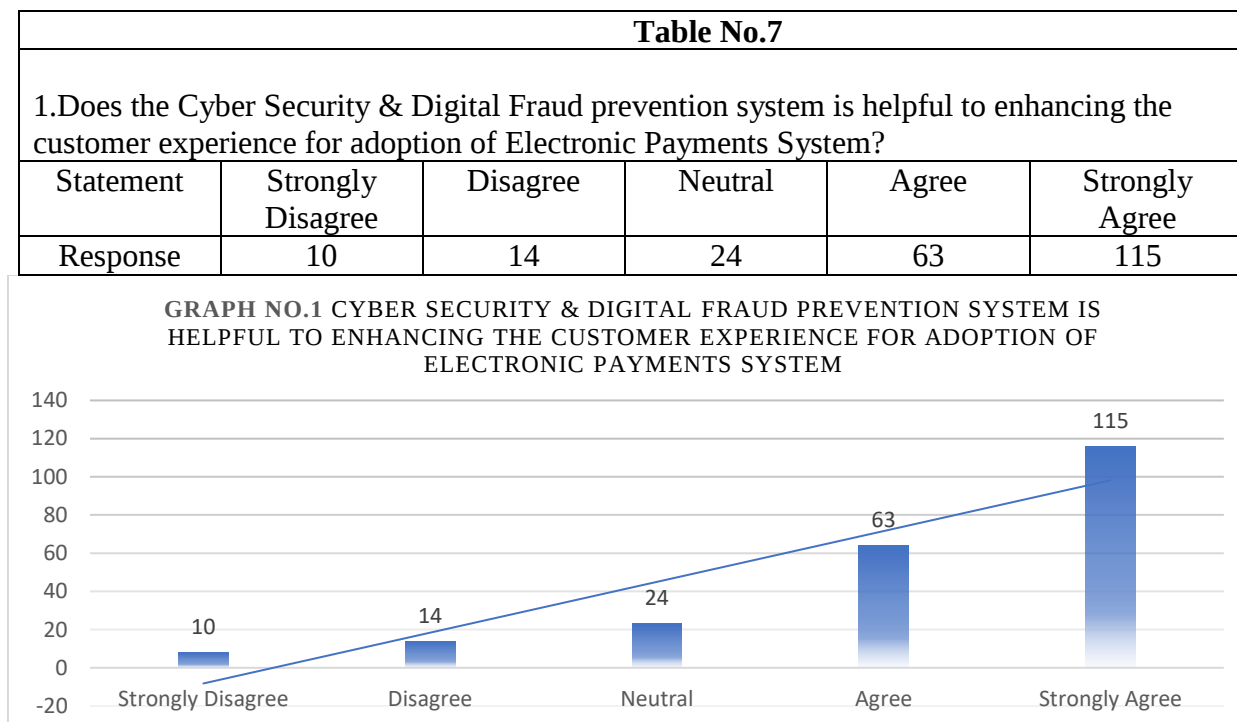
Table No.6				
Income Level	Income Between 2000-20000	Income Between 21000-40000	Income Between 41000-60000	Total numbers of Respondents
Response	75	87	64	226

Interpretation:

The following Table No.6 of income level of the respondents are divided into three categories 2000-20000, 21000-40000 and 41000-60000 thousand INR. Mostly respondent (87) are belongings into the category of the income group of 21000-40000 income group in demographical analysis.

PART B

DESCRIPTIVE ANALYSIS OF DATA

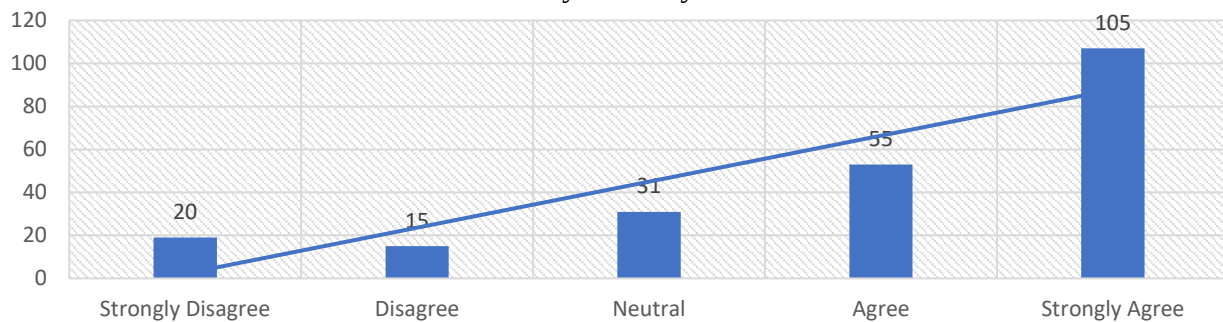


Interpretation:

The findings indicate that a significant majority of the respondents hold a favourable view of the role of Cyber Security and Digital Fraud preventions techniques in digital payments. Specifically, 80.0% of the participants (28.44% Agree and 51.56% Strongly Agree) affirm that Cyber Security prevention systems positively enhance the customer experience associated with electronic payments platforms. Conversely, only 9.78% of the respondents expressed a dissenting opinion (6.22% Disagree and 3.56% Strongly Disagree), reflecting a relative apportion of scepticism. The remaining 10.22% remained neutral, which may imply either limited exposure to Cyber Security preventions-enabled services or uncertainty about their impact. The most frequent response, “Strongly Agree” (51.56%), underscores strong user confidence in preventions technology of c. These insights support the growing consensus in fintech literature that Cyber Security preventions techniques assess consumer awareness of digital payment risks and protections. To evaluate the future growth potential of Electronic Payment Systems in India. To assess consumer awareness of digital payment risks and protections. To evaluate the future growth potential of Electronic Payment Systems in India, can significantly streamline, personalize, and secure the user journey within digital financial systems.

Table No. 8					
2. Does the Cyber Security’s fraud detection and preventions techniques is helpful to enhance the user’s interest for adoption of Electronic Payments System?					
Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Response	20	15	31	55	105

Graph No.2 The Cyber Security's's fraud detection and preventions techniques is helpful to enhance the users interest for adoption of Electronic Payments System.



Interpretation:

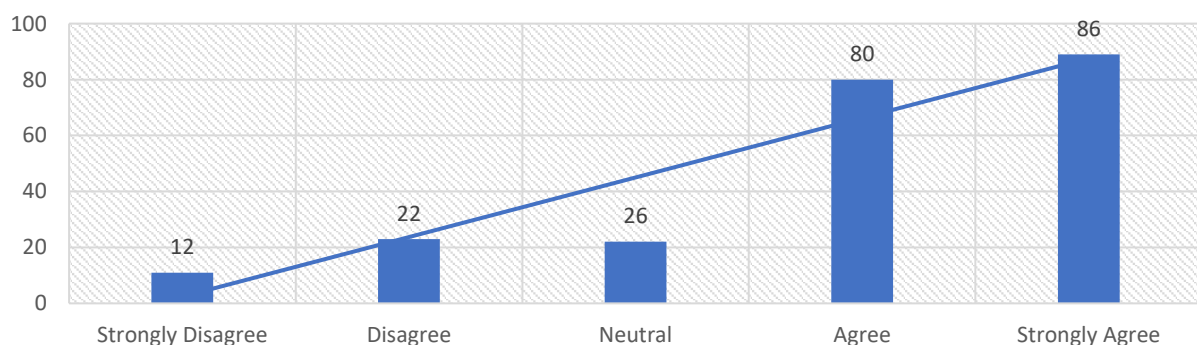
A majority of respondents (107 out of 225, or 47.56%) Strongly Agree that Cyber Security preventions-based fraud detection techniques encourage the adoption of Electronic Payment Systems. 53 respondents (23.56%) Agree, reinforcing the positive sentiment. Together, 71.11% (160 out of 225) of participants have a positive perception. Only 7.56% (17.1%) expressed disagreement (Strongly Disagree + Disagree). 31 respondents (13.78%) are neutral. The data clearly indicates that most users believe preventions-driven fraud prevention with Digital Fraud increases their interest and trust in adopting Electronic Payment Systems. This highlights the importance of integrating secure, intelligent fraud prevention mechanisms to boost user confidence and adoption rates.

Table No. 9

3. Does the block chain technology of Cyber Security and Digital Fraud prevention techniques are improving the user's satisfaction level for adopting of Electronic Payments System?

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Response	12	22	26	80	86

Graph No.3. The Block chain technology of Cyber Security and Digital Fraud prevention techniques are improving the improving the user's satisfaction level for adopting of Electronic Payments System.

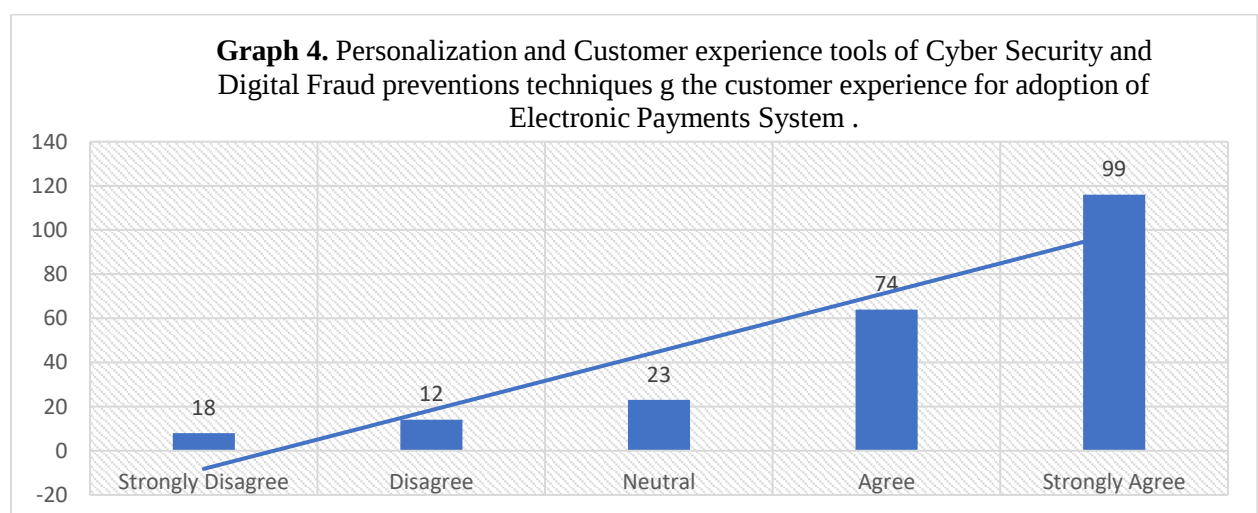


Interpretation:

The analysis highlights that blockchain technology, when integrated with Cyber Security and Digital Fraud preventions tools, significantly contributes to enhancing user satisfaction in the context of Electronic Payment System adoption. Out of a total of 225 respondents, a substantial majority—comprising 35.6% who agreed and 39.5% who strongly agreed—expressed positive views on the impact of blockchain-enabled preventions

tools. This indicates that approximately 75.1% of users perceive these technologies as effective in improving their overall satisfaction with digital transactions. In contrast, only a minor segment of the sample population expressed dissatisfaction, with 10.2% disagreeing and 4.9% strongly disagreeing. Additionally, 9.8% of respondents remained neutral. These findings suggest that the secure, transparent, and decentralized nature of blockchain—combined with the intelligent, adaptive features of Cyber Security and Digital Fraud preventions techniques, helps to build trust and reliability in digital financial platforms.

Table No. 10					
4. Does the Personalization and Customer experience tools of Cyber Security and Digital Fraud preventions techniques has enhanced the customer experience for adoption of Electronic Payments System?					
Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Response	18	12	23	74	99

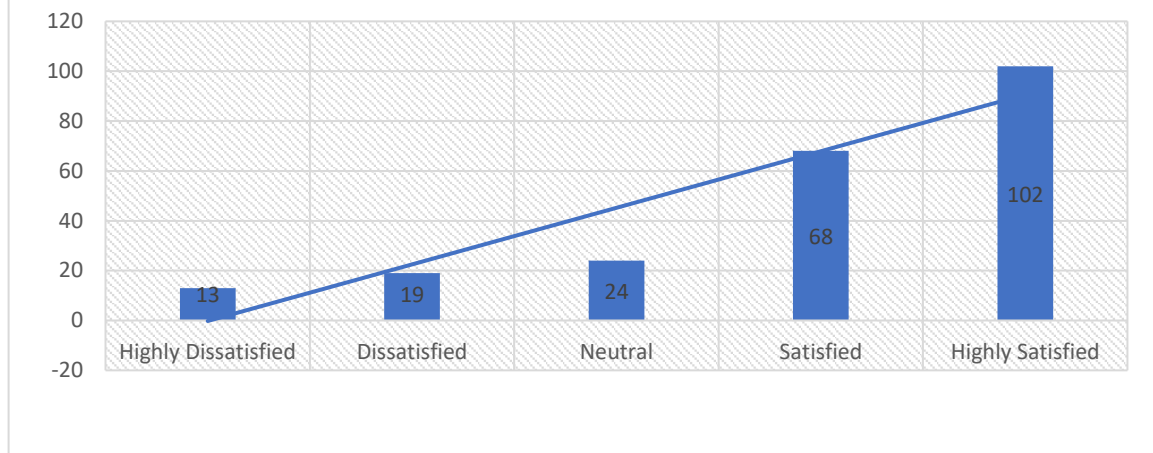


Interpretation:

The findings indicate that a significant majority of the respondents hold a favourable view of the role of Cyber Security and Digital Fraud preventions tools in Electronic Payments. Specifically, 80.0% of the participants (28.44% Agree and 51.56% Strongly Agree) affirm that preventions systems positively enhance the customer experience associated with Electronic Payments platforms. Conversely, only 9.78% of the respondents expressed a dissenting opinion (6.22% Disagree and 3.56% Strongly Disagree), reflecting a relatively small proportion of scepticism. The remaining 10.22% remained neutral, which may imply either limited exposure to Cyber Security preventions-enabled services or uncertainty about their impact. The most frequent response, “Strongly Agree” (51.56%), underscores strong user confidence in Cyber Security and Digital Fraud detection’s role. These insights support the growing consensus in fintech literature that technologies can significantly streamline, personalize, and secure the user.

Table No. 11					
5. Are you satisfied with the Biometric Authentication techniques of Cyber Security and digital Fraud preventions system for solving the problem of adoption of Electronic Payments System with safety and security related measures?					
Statement	Highly Dissatisfied	Dissatisfied	Neutral	Satisfied	Highly Satisfied
Response	13	19	24	68	102

Graph No. 5: Satisfaction level with the Biometric Authentication techniques of Cyber security and Digital Fraud preventions system for solving the problem of adoption of Electronic Payments System with safety and security related measures.



Interpretation:

The survey sought to assess users' satisfaction with the Biometric authentication methods- such as fingerprint, facial recognition and iris detection –integrated through Cyber Security and Digital Fraud detections techniques to address safety and security concerns in Electronic Payments System. The findings indicate a strong positive sentiment among respondents regarding the effectiveness of Cyber Security prevention-driven biometric solutions. Out of the total participants, 49.0% (n = 102) reported being highly satisfied, while 32.7% (n = 68) expressed satisfaction. This cumulatively accounts for 81.7%, suggesting a high level of user confidence in the reliability and security offered by biometric authentication mechanisms. A neutral stance was observed in 11.5% (n = 24) of the participants, indicating a moderate or undecided perception, which may stem from limited exposure or mixed experiences with biometric technologies. On the contrary, only a small fraction exhibited dissatisfaction: 9.0% (n = 19) were dissatisfied, and 6.2% (n = 13) were highly dissatisfied.

CHAPTER NO.5: FINDINGS CONCLUSION SUGGESTIONS LIMITATIONS AND FUTURE RESEARCH SCOPE OF STUDY

5.1 FINDINGS:

The findings indicate that **perceived cybersecurity assurance** plays a significant role in shaping consumer trust and adoption intention toward EPS. Concerns related to **digital fraud, data privacy, and unauthorized access** exert a negative influence on consumer confidence. Trust is found to function as a **critical mediating variable**, linking cybersecurity perceptions and digital fraud risk to adoption behaviour. Furthermore, **digital literacy and awareness of secure payment practices** significantly enhance consumers' willingness to engage in electronic payments. The results also reveal **demographic heterogeneity**, with age, education level, and prior digital payment experience moderating the relationship between perceived risk and adoption intention.

5.2 CONCLUSION:

This study contributes to the electronic payments literature by demonstrating that the success of EPS adoption extends beyond technological efficiency to encompass **perceived security, trust, and fraud-related concerns**. In the Indian context, where digital payment penetration is rapidly expanding, cybersecurity and digital fraud emerge as decisive factors influencing consumer acceptance. The findings underscore the necessity of a **trust-centric and security-oriented digital payment ecosystem**, supported by robust regulatory frameworks and consumer education initiatives. By integrating cybersecurity and digital fraud considerations into consumer adoption analysis, the study offers meaningful theoretical and practical insights for sustaining long-term digital payment usage.

5.3 SUGGESIONS:

From a managerial perspective, payment service providers and financial institutions should prioritize **advanced cybersecurity mechanisms**, including real-time fraud detection, encryption protocols, and multi-factor authentication. Transparent communication regarding security features can significantly strengthen consumer trust. Policymakers and regulators should reinforce **cyber governance frameworks** and promote nationwide **digital financial literacy programs** to mitigate fraud-related apprehensions. These measures are essential for fostering inclusive and secure digital financial adoption.

- **Technological Solutions**

Advanced technologies such as encryption, tokenization, biometric authentication, and artificial intelligence-based fraud detection systems enhance transaction security. Machine learning algorithms can identify suspicious patterns and prevent fraud in real time.

- **Regulatory Frameworks**

Governments and regulatory bodies play a crucial role in establishing cybersecurity standards, enforcing compliance, and promoting secure payment practices. Strong legal frameworks increase accountability and consumer protection.

- **Consumer Awareness and Education**

Educating users about safe digital practices, recognizing fraudulent communications, and protecting personal information is essential. Awareness programs significantly reduce the success rate of social engineering attacks.

5.4 LIMITATIONS AND FUTURE RESEARCH SCOPE

This study is subject to certain limitations. **First**, the findings are based on a **cross-sectional research design**, which restricts causal inference and temporal analysis. **Second**, the use of **self-reported survey data** may introduce response bias. **Third**, the sample is geographically constrained, limiting the generalizability of the results to the broader population. Future research may employ **longitudinal designs**, cross-country comparisons, or experimental approaches to capture evolving consumer perceptions. Additionally, incorporating theoretical lenses such as **UTAUT**, **Protection Motivation Theory**, or **Trust-Risk frameworks** may further enrich understanding of EPS adoption dynamics.

REFERANCES

1. Zhang et al. 2019. Improving data quality for fraud detection in digital payments. Journal of Financial Technology,5(3), 33-47
2. Acquisti A. Brandimarte,L.,& Loewenstein,G.(2015).privacy and human behavior in the age of information Science,347 (621)509-514
3. Electronic Payment Systems Development in a Developing Country: The Role of Institutional Arrangements,<https://www.semanticscholar.org/paper/Electronic-Payment-Systems-Development-in-a-The-of-BriggsBrooks/ff6e27ef208927eac68e1bf5152360bbbcffddaf>
4. IOP Conf. Series: Journal of Physics: Conf. Series <https://iopscience.iop.org/article/10.1088/1742-6596/1140/1/012033/pdf>.
5. Empirical Study on Customer Perception of E-Commerce: Mediating Effect of Electronic Paymenthttps://www.researchgate.net/publication/339774377Empirical_Study_on_Customer_Perception_of_E-Commerce_Mediating_Effect_of_Electronic_Payment_Security.