International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 06 | June – 2025 DOI: 10.55041/ISJEM04355
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

A STUDY ON DEVLOPMENT

OF M-COMMERCE SECURITY FRAMEWORK OF CUSTOMER

Aman Choudhury[1], Dr. Neelima Singh Thakur[2]

[1]Student , Amity Business School, Amity University Chhattisgarh, India
[2]Assistant Professor, Amity Business School, Amity University Chhattisgarh, India

----------***----------

Abstract - The evolution of digital technology has led to a dramatic rise in mobile commerce (M-commerce), enabling users to conduct financial and commercial transactions seamlessly through mobile devices. While M-commerce offers unmatched convenience and accessibility, it also introduces a spectrum of security threats including data breaches, unauthorized access, identity theft, and lack of user trust. These risks underscore the urgent need for a secure and user-centric framework that safeguards customer data and fosters confidence in mobile transactions.

This research paper aims to explore, analyze, and propose a comprehensive **M-commerce security framework** tailored specifically to customer requirements. The study investigates the core components of M-commerce security—such as authentication mechanisms, secure communication protocols, encryption practices, and user data privacy—and emphasizes the integration of these elements into a multi-layered framework. The research employs a **quantitative methodology**, using structured questionnaires to gather data from a sample of 44 respondents. The analysis reveals key factors affecting consumer behavior, perceptions about mobile security, preferred payment methods, and trust-related issues.

The proposed framework not only addresses technical vulnerabilities but also focuses on enhancing user awareness, supporting secure app development practices, and implementing regular updates and security assessments. By incorporating both preventive and detective controls, the framework ensures protection of data integrity, confidentiality, and system availability.

This study offers valuable insights for businesses, developers, and policymakers seeking to strengthen the digital commerce environment. It contributes to the academic discourse on cybersecurity in mobile platforms and serves as a foundational reference for future innovations in secure mobile commerce ecosystems.

Keywords: M-Commerce, Mobile Security, Data Privacy, Authentication, User Trust, Digital Transactions, India

I.INTRODUCTION

Mobile commerce (m-commerce) has rapidly transformed the digital economy by enabling users to conduct financial transactions through smartphones and wireless networks. Its growth in India has been fueled by affordable internet access, digital payment infrastructure like UPI, and increased smartphone penetration. However, this convenience is accompanied by rising security threats, including data breaches, identity theft, and fraudulent transactions.

M-commerce platforms today allow users to purchase goods, pay bills, book tickets, transfer funds, and access a variety of services, all from the convenience of their mobile devices. This ubiquity and convenience have led to a significant rise in mobile-based transactions globally. However, this rapid growth has also been accompanied by a parallel increase in **security vulnerabilities**, posing serious challenges to customer privacy, data protection, and financial security.

Users of M-commerce platforms face numerous threats including identity theft, data breaches, phishing attacks, malware infections, unauthorized access, and transaction fraud. These risks are compounded by the use of unsecure networks, lack of user awareness, and the presence of poorly secured third-party applications. Such threats not only endanger the personal and financial information of consumers but also erode trust in digital systems—trust that is vital for the sustainable growth of M-commerce.

Users of M-commerce platforms face numerous threats including identity theft, data breaches, phishing attacks, malware infections, unauthorized access, and transaction fraud. These risks are compounded by the use of unsecure networks, lack of user awareness, and the presence of poorly secured third-party applications. Such threats not only endanger the personal and financial

information of consumers but also erode trust in digital systems—trust that is vital for the sustainable growth of M-commerce.

The **primary objectives** of the study include:

- Examining the key security aspects associated with M-commerce platforms.
- Identifying the components from existing security frameworks that can be applied to mobile commerce.
- Evaluating customer perception and behavioral patterns related to M-commerce security.
- Designing a practical security model that can be adapted by businesses to foster trust and ensure transaction safety.

Despite technical advancements, many users remain concerned about the safety of their personal and financial data during mobile transactions. Weak authentication protocols, lack of user education, insecure app designs, and insufficient privacy disclosures contribute to low consumer trust in m-commerce platforms. Existing security models often prioritize system-level defenses, overlooking customer-centric concerns.

This study aims to address these gaps by developing a multi-layered, customer-focused m-commerce security framework. Through quantitative analysis of user responses, the research identifies key concerns and preferences, and proposes a structured approach to enhance transaction integrity, privacy protection, and trust in mobile commerce environments.

I.BACKGROUND OF THE STUDY

The proliferation of mobile technologies has led to a profound transformation in the way individuals and businesses interact in the digital ecosystem. Among the most significant developments in this realm is the rise of **Mobile Commerce (Mcommerce)**—a subset of electronic commerce (E-commerce) that enables users to conduct commercial transactions through wireless handheld devices such as smartphones and tablets. M-commerce has reshaped business models, marketing strategies, and customer engagement paradigms, offering real-time, locationindependent, and user-friendly shopping experiences.

However, this convenience and accessibility come with inherent **security risks** that threaten the very trust on which digital commerce thrives. As mobile devices become ubiquitous and increasingly embedded in the everyday lives of consumers, they also become attractive targets for cybercriminals. Incidents of data breaches, phishing attacks, unauthorized access, mobile malware, and identity theft are rising in tandem with M-commerce adoption. In such a dynamic and risk-prone environment, **developing a robust, customer-centric security framework is no longer optional—it is essential**.

II. Review of Literature

The evolution of mobile commerce (m-commerce) has prompted significant academic interest in understanding its adoption drivers, barriers, and security implications. Scholars such as Saifullah Sadi (2021) identified key technological and behavioral factors affecting m-commerce adoption in developing countries. Using models like the Theory of Reasoned Action (TRA) and Technology Acceptance Model (TAM), these studies emphasized perceived risk and trust as central to user engagement.

Haitham Jouda and Emmanuel Nartey (2022, 2023) extended TAM and the Theory of Planned Behavior (TPB) to evaluate mobile banking adoption in Palestine, noting that usability and security significantly impact consumer behavior. Similarly, Sanjay Dhingra (2019) explored mobile banking in India, concluding that security, ease of use, and customer support directly influence adoption intent. These findings highlight that user perceptions of safety are as critical as technical capabilities in determining m-commerce success.

Dr. Shanta Arakari (2021) and Mohamad Habli (2022) reinforced the importance of secure payment channels, transparent privacy policies, and encryption in building user trust. However, much of the existing literature remains developer-focused and lacks a comprehensive, user-oriented security framework tailored for mobile platforms. This study addresses that gap by proposing a customer-centric security model that integrates technical safeguards with behavioral and trustenhancing components.

III. Research Methodology

3.1 Research Design

This study adopts a **quantitative, descriptive research design** aimed at analyzing user perceptions and concerns regarding m-commerce security. The approach enables statistical interpretation of user behavior and the identification of key elements necessary for a customercentric security framework.

International Scientific Journal of Engineering and Management (ISJEM)
Volume: 04 Issue: 06 | June – 2025
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata
ISSN: 2583-6129
DOI: 10.55041/ISJEM04355

3.2 Sampling Technique

The sample consisted of **47 respondents**, selected using **simple random sampling** to ensure unbiased representation.
Participants included users from diverse age groups, educational backgrounds, and occupational sectors who actively engage in mobile commerce transactions.

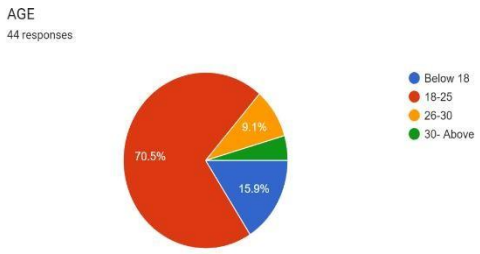
3.3 Data Collection

Primary data was collected through a **structured questionnaire** circulated via Google Forms. The questionnaire covered demographic information, usage patterns, perceived security risks, preferred payment methods, and trust factors in mcommerce environments.

3.4 Data Analysis

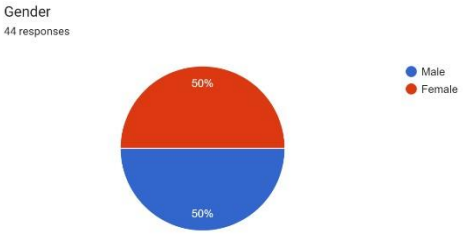
Data was analyzed using percentage-based frequency analysis and interpreted through bar graphs. This helped in understanding the distribution of responses related to mcommerce usage, perceived risks, and user expectations regarding security features.

1- AGE GROUP



Interpretation:
From the given responses we get to know that out of 44 respondents 70.5% belongs to 18-25 age group, 9.1% belongs to 25-30 age group, 4.5 % belongs to respondents who are more than 30 years old. And also we find that 15.9% respondents comes under below 18 age group

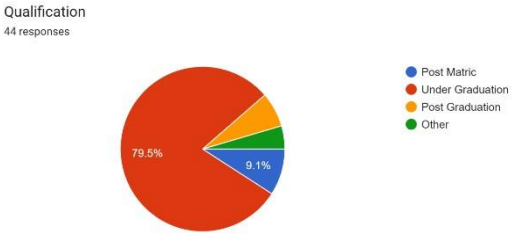
2 - GENDER



Interpretation:

From the given responses we get to know that out of 44 respondents ,50% are female and 50% are male.

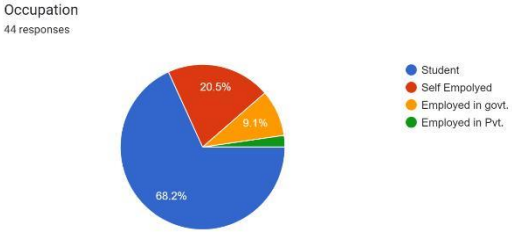
3-Qualification



Interpretation-

From the given response we get to know that 79.5% of respondents are under graduate 6.8 % of respondents are post graduate. 9.1%are post matric and 4.5% are others .

4 – Occupation

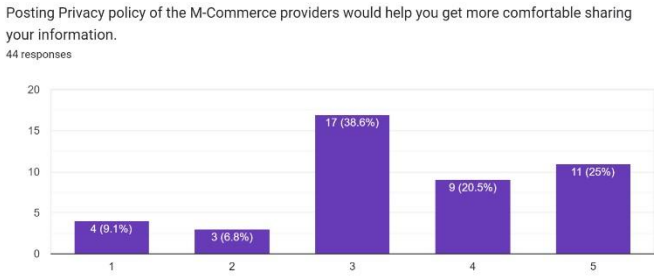


Interpretation:

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 06 | June – 2025 DOI: 10.55041/ISJEM04355
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

From the given response we get to know that 68.2% are students , 9.1% are government employee , 2.3% are employed in the private sector , 20.5% are selfemployed.

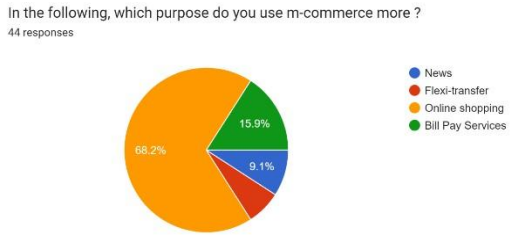
5.Posting Privacy policy of the M-Commerce providers would help you get more comfortable sharing your information.



Interpretation:

From the given responses we get to know by the average method 3 =38.6% therefore most of the response are comfortable for sharing their information

6.In the following, which purpose do you use mcommerce more:

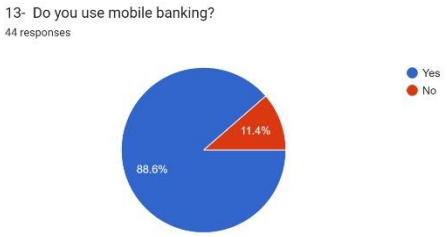


Interpretation:

From the given responses we can clearly analyse that 68.2% are using only for online shopping , 15.9 % are using for bill pay service, 9.1 % are using for news, 6.8% are using for only flexi –transfer,.

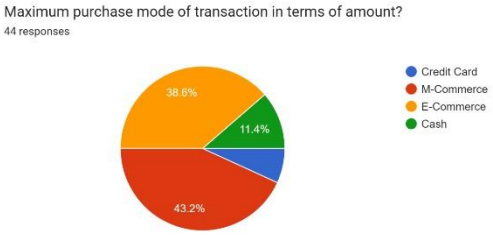
7. Do you use mobile banking?

From the given responses we can clearly analyze that



88.6% are using mobile banking and only 11.4% are not using mobile banking.

8. Maximum purchase mode of transaction in terms of amount?



Interpretation:

From the given response we get to know 6.8% are using credit cards, 43.2% are using M commerce, 38.6% are using E commerce and 6.8% are using cash

3.5 Tools Used

The primary statistical tool used was percentage analysis, which is suitable for identifying trends and summarizing survey responses. The formula used was: Percentage = (Number of Respondents for a Response / Total Respondents) × 100 4. Results and Analysis

IV. Results and Analysis

4.1 Demographic Profile

Out of the 47 respondents, the majority (70.5%) belonged to the 18–25 age group, indicating that young adults are the primary users of m-commerce. Gender distribution was equal (50% male, 50% female), and 79.5% were undergraduates, highlighting high engagement among educated youth. In terms of occupation, 68.2% were students, followed by 20.5% self-employed, reflecting mcommerce's popularity among digitally active populations.

4.2 Usage Patterns and Preferences A significant **69.8% of users preferred UPI** as their primary payment mode, followed by 25.6% using net banking. Online shopping was the most common activity (68.2%), while bill payments and information services were less frequent. 88.6% of respondents use mobile banking, indicating widespread integration of digital finance tools.

4.3 Perception of Security

When asked about the urgency of enhancing m-commerce security, 38.6% said "Yes," while another 38.6% selected "Maybe," revealing moderate awareness but high concern. About 29.5% of users cited "lack of technical support" as the main barrier, followed by concerns over data safety (27.3%) and unfamiliarity with technology.

4.4 Trust and Privacy Considerations On a Likert scale (1–5), 38.6% of respondents gave a neutral score (3) regarding comfort with sharing personal data—even when privacy policies were posted— indicating partial trust. Moreover, most users rated "Trust" as a critical factor in m-commerce, with over 25% assigning it a score of 9 or 10, confirming its importance in driving adoption.

4.5 Perceived Trends in India

When asked about the trend of m-commerce usage in India, 29.5% perceived it as rising, while 27.3% saw it as constant, and 22.7% viewed it as declining. This split indicates awareness of growth potential, but also lingering doubts about security and reliability.

V. Findings and Discussion

5.1 Key Findings

1. **High Adoption Among Youth**

   The study reveals that m-commerce is predominantly used by young adults (aged 18–25), especially students and undergraduates. This age group demonstrates both high engagement and reliance on mobile-based digital services such as UPI payments and online shopping.

2. **UPI as the Preferred Payment Mode**

   A substantial 69.8% of respondents preferred UPI over other payment methods like net banking and e-wallets. This indicates a strong shift toward real-time, low-cost digital payment solutions enabled by mobile apps.

3. **Security and Trust as Critical Concerns**

   Security concerns were prominent, with 38.6% of participants explicitly identifying the need for improved m-commerce security. The leading barriers to adoption were lack of technical support (34.1%) and fear of data misuse (29.5%), showing that users are aware of the risks but often feel unequipped to manage them.

4. **Moderate Trust in M-Commerce Platforms**

   Although respondents used m-commerce widely, there was hesitation in fully trusting platforms. Many users remained neutral when asked if privacy policies made them more comfortable sharing data, indicating a gap between privacy policy presentation and user assurance.

5. **Need for Customer-Centric Security**

   The findings underscore that existing security frameworks may not adequately address end-user concerns. Users want clear, accessible, and actively enforced security mechanisms—such as biometric authentication, encryption, and realtime fraud alerts—rather than passive policies.

5.2 Discussion

The results affirm that m-commerce has significant potential in India, particularly among younger demographics. However, the absence of user-friendly and transparent security mechanisms remains a major impediment to full-scale adoption. While users are digitally capable and transaction-ready, their willingness to trust mobile platforms depends heavily on visible, reliable, and easy-to-understand security features. This aligns with prior research (e.g., Jouda & Nartey, 2022; Sadi, 2021), which emphasizes that adoption of mobile commerce is strongly tied to perceived security and trust. Furthermore, the data supports the argument that technical advancements alone are not enough—behavioral reassurance, user awareness, and proactive communication play equally vital roles. In the Indian context, where users come from varied socio-economic and educational backgrounds, a **hybrid approach combining technical security with usercentric design** is critical. The study therefore recommends a layered framework that not only encrypts data and authenticates identity but also educates users, reinforces trust through UI/UX elements, and makes privacy policies more meaningful and transparent.
read as far as the abstracts. If they try to go ready there this point, they are routinely asked, whether they would like to order the pdf, and are given directions as to how to do so.

CONCLUSIONS

In today's rapidly evolving digital economy, **mobile commerce (m-commerce)** stands at the forefront of technological innovation, transforming the way consumers interact with businesses and conduct financial

transactions. With its unparalleled convenience, accessibility, and real-time functionality, m-commerce has redefined the boundaries of commerce—empowering individuals with the ability to shop, pay, bank, and invest from virtually anywhere. However, as this paradigm shift accelerates, so too does the complexity of **cybersecurity threats** and **privacy concerns**.

This research project has thoroughly explored the **development of a robust security framework for mcommerce**, particularly from a customer-centric perspective. Through a combination of **primary research**, **literature review**, and **statistical analysis**, the study has uncovered several important insights regarding user behavior, security expectations, and the vulnerabilities present in the current m-commerce ecosystem.

The findings of the research indicate that while mcommerce adoption is on the rise—particularly among young and tech-savvy consumers—there exists a significant gap in **user awareness**, **technical support availability**, and **confidence in data protection mechanisms**. Many users reported hesitation in fully adopting m-commerce due to fears related to data breaches, identity theft, and lack of transparent security policies. Notably, the survey revealed that a substantial portion of participants felt unsure about the security features of the platforms they were using, and a majority demanded stronger authentication, regular security updates, and better support for secure transactions.

ACKNOWLEDGEMENT

I would like to express my deepest gratitude to all those who contributed to the successful completion of this research project titled **"Development of M-Commerce Security Framework of Customer."**

First and foremost, I am sincerely thankful to my project supervisor, **Dr. Neelima Singh Thakur**, for her continuous guidance, encouragement, and invaluable support throughout this project. Her insightful feedback, patient mentoring, and expert knowledge provided the foundation upon which this research was built. I also extend my heartfelt thanks to **Dr. Sumita Dave**, Director of Amity Business School, for providing the institutional support and academic environment necessary for carrying out this work.

I would also like to acknowledge the invaluable help and cooperation of the **respondents** who participated in the survey. Their responses provided the empirical backbone for the analysis in this study.

Special thanks are due to my **parents and friends** for their moral support, patience, and motivation throughout the process. Their encouragement has been instrumental in keeping me focused and determined to complete this work within the given time frame.

Lastly, I thank **Amity University, Chhattisgarh**, for offering me this opportunity and providing the resources to carry out this research. This project has been an incredible learning experience, and I am truly grateful to everyone who played a role in its completion.

REFERENCES

- Sadi, S. (2021). *Factors Affecting the Adoption of Mobile Commerce in Malaysia: A Study Based on Technology Models.* International Journal of Mobile Computing and Multimedia Communications.
- Jouda, H., & Nartey, E. (2022). *Expanding the Technology Acceptance Model for Mobile Banking Adoption in Palestine.* Journal of Financial Services Research, 38(2), 115–130.
- Jouda, H. (2023). *A Cross-Sectional Study on Mobile Banking Usage and Security Perceptions.* Journal of Mobile and Ubiquitous Systems, 11(1), 45–59.
- Dhingra, S. (2019). *Mobile Banking Adoption in India: A Customer-Centric Approach Based on TAM.* Indian Journal of Economics and Business, 18(3), 81–92.
- Habli, M. (2022). *M-Commerce Adoption Among Higher Education Students in Palestine: An Extended TAM Approach.* International Journal of E-Business Research, 18(4), 59–75.
- Soliman, M., & Khalid, J. (2020). *M-Commerce Applications and User Behavior: Comparative Study in Emerging Markets.* Mobile Commerce Research Journal, 14(2), 122–137.
- Arakari, S. V. (2021). *The Impact of Mobile Commerce on Indian Retailers and Consumers.* Journal of Retail and Consumer Services, 25(2), 33– 40.
- Davis, F. D. (1989). *Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology.* MIS Quarterly, 13(3), 319–340.
- Ajzen, I. (1991). *The Theory of Planned Behavior.* Organizational Behavior and Human Decision Processes, 50(2), 179–211.