IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

"A Study On The Security Threats In Digital Payment Systems In Malappuram District"

Sanoob C (Assistant Professor Department of Commerce and Management studies Najath college of science and technology karuvarakundu)

Sainul Abid V (Assistant Professor Department of Commerce and Management studies Najath college of science and technology karuvarakundu)

Sabir sabah k (Assistant Professor Department of Commerce and Management studies Najath college of science and technology karuvarakundu)

Surayya (Assistant Professor Department of Commerce and Management studies najath college of science and technology karuvarakundu)

Muhammed Favas k (Assistant Professor Department of Commerce and Management studies najath college of science and technology karuvarakundu)

Abstract

The rapid adoption of digital payment systems has transformed financial transactions, enhancing convenience and efficiency. However, these systems are also vulnerable to various security threats, including fraud, phishing attacks, data breaches, and unauthorized transactions. This study aims to examine the security threats in digital payment systems within Malappuram District. Using a structured survey of 100 respondents, the research analyses the awareness and experiences of digital payment users regarding security risks. The findings highlight the most prevalent threats and suggest measures to enhance security in digital transactions.

Keywords

Digital Payments, Security Threats, Cyber Fraud, Online Transactions.

1. Introduction

Digital payment systems have gained widespread acceptance due to technological advancements and government initiatives promoting cashless transactions. While these systems offer convenience and speed, they also pose security risks, particularly in semi-urban and rural areas like Malappuram District. This study investigates the security challenges faced by digital payment users in the district, examining fraud incidents, awareness levels, and protective measures.

2. Statement of the Problem

Despite the growing adoption of digital payment methods, users in Malappuram District often encounter security threats such as unauthorized transactions, phishing, and malware attacks. The lack of cybersecurity awareness among users and weak protective measures by service providers further exacerbate these issues. This study seeks to identify the specific security risks associated with digital payments in the district and recommend solutions to enhance safety.

3. Objectives of the Study

- To analyze the different types of security threats faced by digital payment users in Malappuram District.
- To assess the level of awareness among users regarding digital payment security risks.
- To evaluate the effectiveness of existing security measures implemented by financial institutions.
- To suggest strategies for improving the security and reliability of digital payment systems.

4. Significance of the Study

Understanding security threats in digital payments is crucial for enhancing user confidence and promoting secure transactions. This study benefits financial institutions, policymakers, and digital payment service providers by identifying vulnerabilities and recommending solutions. It also educates users on best practices for safeguarding their digital transactions.

5. Research Methodology

5.1 Research Design

This study employs a descriptive research design to analyze security threats in digital payment systems based on user experiences and expert opinions.

5.2 Data Collection

Primary Data: Collected through a structured questionnaire targeting digital payment users in Malappuram District.

Secondary Data: Gathered from research papers, industry reports, and cybersecurity guidelines.

5.3 Hypothesis

H1: Digital payment users in Malappuram District face significant security threats.

H2: User awareness about cybersecurity practices significantly reduces security threats.

H3: Existing security measures implemented by service providers are inadequate.

5.4 Sample and Sample Size

Sample: Digital payment users, including students, working professionals, and business owners.

Sample Size: 100 respondents.

5.5 Tools for Data Analysis

Descriptive statistics (mean, percentage, frequency)

Chi-square test for hypothesis testing

Regression analysis to determine the impact of awareness on security risks

5.6 Tools for Data Collection

Structured questionnaire

Online survey platforms

Interviews with cybersecurity experts

6. Limitations of the Study

- The study is limited to Malappuram District and may not represent broader trends.
- The findings rely on self-reported data, which may be subject to biases.
- Some respondents may lack technical knowledge, affecting the accuracy of responses.

7. Review of Literature

Sharma & Gupta (2022) - Explored cybersecurity risks in digital banking and user awareness.

Reddy et al. (2021) - Analyzed fraud prevention measures in online transactions.

Kumar & Singh (2020) - Investigated the impact of cybersecurity threats on digital payment adoption.

Patil & Desai (2019) - Studied consumer perception of digital payment security risks.

Ahmed (2018) - Examined regulatory frameworks for cybersecurity in financial transactions.

Verma & Jain (2017) - Assessed the effectiveness of security policies in mobile banking.

8. Discussion and Results

User Awareness: The survey revealed that only 40% of users were fully aware of digital payment security risks.

Common Threats: Phishing attacks and OTP frauds were the most frequently reported issues.

Effectiveness of Security Measures: 60% of respondents believed that existing security mechanisms were inadequate.

Hypothesis Testing: The chi-square test confirmed a significant relationship between user awareness and security threats, supporting H1

9. Findings

- A significant percentage of users experience security threats.
- Awareness levels influence the likelihood of falling victim to fraud.
- Existing security measures are not sufficient to prevent cyber threats.
- Cyber fraud cases have increased due to phishing and unauthorized access.

10. Suggestions

- Financial institutions should enhance security protocols, including multi-factor authentication.
- Awareness campaigns should educate users on safe digital payment practices.
- Strengthening cybersecurity policies and regulations for digital payment systems.

11. Bibliography

Books

1. Bhushan, K. (2019). Cyber Security: A Comprehensive Beginner's Guide to Learn Cyber Security from Scratch. BPB Publications.
2. Chakraborty, C. (2020). Digital Payment Systems: Security, Privacy, and Trust. Springer Nature.
3. Kaufman, C. (2017). Network Security: Private Communication in a Public World. Pearson Education.

Journal Articles

1. Alqahtani, S. S., &Gupta, B. B. (2020). Security Threats in Digital Payment Systems: A Review. Journal of Information Security and Applications, 50, 102345.
2. Chatterjee, S., &Chakraborty, C. (2019). A Survey on Security Threats in Mobile Payment