



# Legal Research Development

An International Refereed e-Journal

ISSN: 2456-3870, Journal home page: <http://www.lrdjournal.com>

Vol. 10, Issue-II, Dec. 2025



## Credit and Debit Card Fraud in the Digital Era: An Analytical Study with Special Reference to Madhya Pradesh

Jyoti Kaushik<sup>a,\*</sup>, 

<sup>a</sup>LL.M. Business Law, Gwalior Law College, Jiwaji University, Gwalior, Madhya Pradesh (India).



### KEYWORDS

Digital Payments, Credit Card Fraud, Debit Card Fraud, Cybersecurity, Financial Crime, Online Transactions, Consumer Awareness, Banking Security, Digital Banking, Madhya Pradesh.

### ABSTRACT

Digital payment systems are evolving at a rapid pace, and credit and debit cards are a crucial component of today's economy. These technological advancements have helped consumers and financial institutions make the process easier, faster and more convenient; but they have also created a variety of card-related crimes. An attempt is made in the present study to have a brief look on the nature, trends and challenges of credit/debit card fraud in digital era with special reference to Madhya Pradesh. The research focuses on the reasons behind fraudulent activity like phishing attacks, skimming, identity theft, data breaches and unauthorized online transactions. It also assesses the awareness among card users, security measures implemented by banks and role of regulatory framework in financial fraud prevention. The method that is used in this research is analysis and description, where the data sources used are primary and secondary data. The results indicate that the extent businesses are becoming digital, cybersecurity awareness about them is not parallel, and this has resulted in an increasing number of fraud cases related to cards. The study underscores the need to strengthen security measures, continuously educate consumers, and implement a collaborative approach involving financial institutions, regulators, and technology vendors to enhance the security of digital payments. The findings provide insights into the changing dynamics of card fraud and actionable insights to reduce risks in Madhya Pradesh and other new digital economies.

## 1. Introduction

The digital revolution has transformed the global financial scene and the way people and businesses conduct their business. Rapid and widespread adoption of digital payment systems has greatly contributed to financial inclusion and monetary transactions in India. Credit cards are now a popular and convenient method of payment for consumers

that are more readily available and secure.

Improved access to banking services, Internet and mobile phones has also contributed to increase card-based transactions in rural and urban areas. (RBI, 2024)

The Government of India has actively promoted Digital payments through various initiatives such as Digital India, Unified Payment Interface (UPI), and

### Corresponding author

\*\*E-mail: [jyotisheopur108@gmail.com](mailto:jyotisheopur108@gmail.com) (Jyoti Kaushik).

DOI: <https://doi.org/10.53724/lrd/v10n2.4>

Received 10<sup>th</sup> Oct. 2025; Accepted 20<sup>th</sup> Nov. 2025

Available online 30<sup>th</sup> December 2025

2456-3870/©2025 The Journal. Publisher: Welfare Universe. This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/)

 <https://orcid.org/0009-0008-1294-550X>



the push towards a Cashless Economy. A result of this is that electronic payment methods have experienced a tremendous increase during the past decade. These are parallel to the continued importance of credit and debit cards in retailing and e-commerce transactions as well as financial services. The ease of using these cards has prompted the consumers to move away from the traditional cash transaction methods to digital payment methods (National Payments Corporation of India [NPCI], 2024).

## **1.1 The background to the study is given**

### **1.1.1 Evolution of Digital Payments in India**

Since the dawn of e-banking in the late 90s, the digital payment ecosystem in India has come a long way. With the rise of internet technology, mobile banking, and payment gateways, consumers are able to make financial transactions with ease. The government has also been actively promoting financial digitization and improving banking infrastructure, further strengthening digital payments. The COVID-19 pandemic also caused a shift towards contactless and online transactions, resulting in an unprecedented surge in digital payments around the country (World Bank, 2022).

### **1.1.2 Rise of credit card/debit card spending**

The credit and debit cards have an important role in today's financial transactions. To satisfy the demand for easy payment solutions, commercial banks and financial institutions have gone all out to increase the number of cards issued. This trend of adopting card payments in retail stores, online marketplaces, and service sectors has played a major role in its widespread adoption. Consumers are adopting cards for everyday use with the benefits such as reward

programs, ease of payment and dependency on cash. This increase in card use aligns with the overall digital transformation happening in India's financial system (RBI, 2024).

### **1.1.3 Problem of the Card-related frauds**

Digital Payment technologies have made transactions easier but also paved the way for cybercriminals. Card related fraud is one of the most significant issues for banks, businesses and consumers. With the surge of digital payments, fraudulent activities like phishing, card skimming, identity theft, data breaches, account takeover and unauthorized transactions online have also surged. With the evolution of technology, cybercriminal techniques are evolving as well, constantly exploiting technology vulnerabilities and human error. This poses a great challenge for financial institutions to protect their customer data and uphold confidence in digital payment systems (Kumar & Gupta, 2023).

Card fraud doesn't just have monetary consequences, it can also damage customer confidence in online banking. Therefore, it is essential for the policy makers, financial institutions and cybersecurity experts to be aware of the why, how and how to prevent card fraud.

### **1.1.4 Significance of the study of Fraud in Madhya Pradesh**

In recent times, Madhya Pradesh, a big state in India, has witnessed huge growth in the usage of digital banking and electronic payment systems. Internet usage, government policy to encourage electronic transactions, and expansion of the banking network have prompted the residents to use credit/debit cards for many things. But this quick

digitalization has also brought along with it new cyber threats and fraudulent practices.

Due to the socio-economic factors, different levels of digital literacy across Madhya Pradesh affecting susceptibility to credit and debit card fraud, the educational significance of credit and debit card fraud in the state is particularly relevant. Understanding the nature of card fraud in the state can provide valuable information about user awareness, what kinds of fraud are taking place, security concerns and how well fraud is being prevented. The findings of such a study can be used by financial institutions, governments and law enforcement agencies to develop a more targeted strategy to increasing the awareness of cyber security and protecting consumers from financial crimes.

As digital payment methods are becoming more common, it is essential to have a thorough knowledge of credit and debit card fraud in Madhya Pradesh to ensure the safe and sustainable development of the digital economy.

## **1.2 Conceptual Framework**

Conceptual framework is the theoretical framework that provides understanding of the important concepts and variables that are related to the research study. To think about payment card fraud, it is important to know the nature of payment cards, the nature of fraud and the relationship between digital financial transactions and cybercrime. These can be applied to explain how technological developments in the banking sector have increased the opportunity for financial convenience and financial crime.

### **1.2.1 Meaning of the Credit cards**

A credit card is a card issued by a bank or financial institution which permits the card holder to pay with credit for purchases of goods and services within a specified amount. There is no requirement for the cardholder to pay immediately on purchase like cash, unlike cash transactions. Instead, the issuing institution pays the merchant on behalf of the buyer and the buyer repays the purchase either all at once or in instalments over a period of time. Credit cards are now a popular financial instrument and have become an indispensable part of the financial landscape as they are convenient, flexible and accepted both domestically and internationally (Reserve Bank of India [RBI], 2024).

Credit cards are also useful for a number of reasons such as reward schemes, cash back, purchase protection and emergency financing. But their widespread usage in online and offline transactions has also made them vulnerable to unauthorized access, identity theft and fraudulent transactions. In the digital commerce age, the security of credit card transactions is a very important issue, especially for financial institutions and consumers (Kumar & Gupta, 2023).

### **1.2.2 Meaning of Debit Cards**

A debit card is one of the payment cards that allows the user to withdraw or use the funds directly from his bank account. Unlike credit cards, debit cards do not involve borrowing money from the card issuer. At the time of purchase/cash withdrawal the amount of the transaction is immediately deducted from the cardholder's savings account or current account. However, Debit Cards are an excellent substitute to cash and are widely adopted by consumers as they can control their expenditures according to their

means (RBI, 2024).

Debit cards are gaining popularity in India, due to the rising banking penetration, financial inclusion initiatives, and digital payment initiatives. Debit cards are used in a point-of-sale terminal, an automated teller machine (ATM) or an online payment gateway to make a purchase. Even though they are convenient, the holders of a debit card are vulnerable to security threats like card skimming, phishing attack, unauthorized access of cards or accounts that might lead to monetary loss if proper precautions are not taken (Singh & Sharma, 2022).

### 1.2.3 Definition of Fraud

Fraud is the intentional act of deception for the purpose of causing financial loss to another party, institution, organization or entity and/or financial gain. It involves knowingly misleading, lying, concealing or distorting information or to gain some advantage. There are various types of fraud including financial fraud, forgery, cyber fraud, banking fraud and identity theft. It is the intention to deceive another party for some economic benefit that is the key factor in fraud (Association of Certified Fraud Examiners [ACFE], 2024).

Banking and financial services fraud typically involves unauthorized use of financial tools or resources, or manipulation of financial information in a transaction, or misuse of financial payment tools. Fraud has also evolved from the more traditional methods to highly sophisticated and technologically advanced fraud schemes, as the financial services industry has evolved into a more digital space. Financial fraud leads to monetary loss as well as loss of trust and credibility amongst consumers and financial institutions (Button &

Cross, 2017).

### 1.2.4 Digital Financial Fraud and Cybercrime

Digital financial fraud is a term that describes any fraud that is done using digital mediums like online banking, mobile applications, digital payment systems, internet-based financial transactions and electronic platforms. It includes many illegal activities like phishing, card skimming, malware attacks, ID theft, Account takeover, Fake websites and unauthorized e-transactions. As digital financial services have increased, so has the opportunity for cybercriminals to take advantage of technological vulnerabilities and human errors (Interpol, 2023).

The term cybercrime is a more general term that is used to describe any criminal activity that uses computers, digital devices, networks or the internet. Financial cybercrime is a crime focused on banking systems, payment networks and digital consumers that aims to obtain sensitive information or financial assets. One of the most important types of financial cyber-enabled crime is credit and debit card fraud, with fraudsters often using digital tools and communication technologies to obtain card details to make fraudulent transactions (United Nations Office on Drugs and Crime [UNODC], 2023).

The link between digital financial fraud and cybercrime is inextricable and in the digital world, the importance of this relationship has continued to rise. Cybercriminals have a larger attack surface thanks to the fast-growing e-commerce, internet banking and electronic payment systems. As a result, governments, regulators, financial institutions, and cybersecurity agencies are redoubling their efforts to fortify security protocols, boost customer awareness, and adopt sophisticated

fraud detection tools. Therefore, it is crucial to understand the characteristics of financial fraud in the digital space to be able to craft effective solutions to safeguard consumers and maintain the integrity of digital payment systems (World Bank, 2022).

The conceptualization of the present study is based on credit card usage, debit card usage, the adoption of digital payments, the nexus between digital payment adoption and cybercrime risks, as well as the nexus between digital payment adoption and frauds in financial activities. The study is aimed at analyzing cause, pattern and preventive measures of 'Credit Card Fraud' and 'Debit Card Fraud' as a whole.

### **1.3 The need and significance of the study**

Information and communication technology (ICT) has been transforming the financial sector and making the world go digital when it comes to payments. Several facilities like internet, smart phone, banking etc. have made e-transactions part and parcel of the economic activities of the people and the country by large. The use of credit and debit cards is a widely adopted method of payment for safe and convenient transactions by consumers and businesses alike. But as more and more people have turned to digital payment, there is more risk for financial fraud and cybercrime. Hence the need to delve into the issues, problem and challenges of Credit Card and Debit Card related frauds particularly in the context of emerging digital economy of Madhya Pradesh.

#### **1.3.1 Dependence on Digital Transactions**

The digital transformation of financial services has had a huge impact on consumers' payment habits.

Electronic payment methods have become popular due to their various advantages, including convenience, speed, accessibility, and decrease in cash transactions. Various initiatives taken by the Government such as Digital India, Financial inclusion etc. and internet banking services has expanded the penetration of Digital Payment systems both in urban and rural areas. Consequently, millions of consumers are now using credit and debit cards for retailing, e-commerce, payment of utilities and banking (Reserve Bank of India [RBI], 2024).

Digital transactions have increased to such an extent that it has created a very connected financial ecosystem. This change has made economic efficiency better, but also presented new security concerns. Increasing reliance on digital payment tools brings with it an increased risk for unauthorized access, data theft, and fraudulent transactions. As a result, knowledge of the risks of card-based payment systems is crucial for payment security and sustainability of digital financial services (World Bank, 2022).

#### **1.3.2 The rate of card fraud is increasing**

The electronic payment system has expanded and so has the amount of credit and debit card financial fraud. These cybercrime techniques have been utilized to acquire sensitive financial data, such as phishing, card skimming, ID theft, malware attacks, social engineering, and illicit online transactions. These fraudulent activities have become more sophisticated, with technological advances and the availability of digital communication platforms (Interpol, 2023).

The financial institutions in India are still grappling

with a serious issue to prevent and detect card related frauds as per the latest reports. The fraudsters frequently exploit consumers' carelessness and the lack of cyber security and technological gaps in digital payment systems. The significance of card usage is also growing with the understanding of card fraud, its causes, patterns and mechanisms of card fraud can help in developing effective prevention and mitigation strategies (Kumar & Gupta, 2023).

### **1.3.3 Financial and Psychological Impact on the Victims**

Fraud associated with credit and debit cards can have a serious financial impact on individuals, businesses and financial institutions. Many victims end up with out-of-pocket direct losses as a result of the unapproved transactions, and recovery and additional costs as a result of the fraud work itself. The Association of Certified Fraud Examiners (ACFE, 2024) reports that fraud can negatively affect individuals' credit scores, financial plans, and other long-term economic issues for those involved in the fraud.

Besides monetary loss, there can be psychological and emotional distress felt by the victim. Suffering from fraud can result in anxiety, stress, fear and frustration, and in a lack of trust in online financial systems. Fraud victims tend to be hesitant to bank online or use electronic payments. This can create hindrances in achieving the broader objective of creating a safe and inclusive digital economy. Hence, it is important to know the multi-dimensional nature of card fraud to formulate a consumer protection measures package (Button & Cross, 2017).

### **1.3.4 Consumer Awareness and Policy Interventions**

The most effective strategy to fight credit and debit card fraud is to raise consumer awareness and enhance regulatory measures. User ignorance of cybersecurity practices, safe methods to transact, password management and fraud detection techniques is the cause of numerous fraud incidents. Ensuring that consumers are aware of the potential risks and preventive measures can help minimize their exposure to fraudulent activity (RBI, 2024).

Besides consumer awareness, it is crucial to ensure comprehensive policy and regulatory frameworks are in place to enhance the security of digital payment systems. To facilitate advanced fraud detection systems, strengthen cybersecurity infrastructure and bestow effective grievance redressal mechanisms, there is a need for co-operation between financial institutions, government agencies, law enforcement authorities and technology providers. The policy measures should focus on strengthening consumer protection, raising consumer awareness of digital payment technologies and holding all players involved in the digital payment space to account (United Nations Office on Drugs and Crime [UNODC], 2023).

The present study is likely to be significant in its endeavour to study the credit card and debit card fraud in the specific context of Madhya Pradesh. As the use of digital payments has increased in the state it is essential to know the motivating factors behind this fraud, knowledge of the fraud among consumers and preventative measures being implemented. This research could provide policy, financial institutions, cybersecurity practitioners,

and consumers with recommendations to help create safer and more resilient digital financial systems.

## 2. Review of Literature

The literature review aids in comprehending the existing academic and institutional studies on credit/debit card fraud, cyber financial crimes and security of digital payments. The increase of electronic banking, online shopping, mobile banking and digital financial services in developed and developing economies has led to card fraud becoming a serious issue according to the previous studies.

### 2.1 Card Fraud National & International studies

Previous studies on card fraud have primarily concentrated on the evolution of fraud techniques and the technology adopted to detect frauds. Button and Cross (2017) claim that traditional financial crimes are now being transited to the online environment, financial criminals are using electronic means to deceive their victims and obtain a financial benefit. It is a statement on the need to recognize that cyber fraud is not a technical issue alone, but a social and psychological issue due to the financial losses, emotional impact and loss of confidence in digital systems that victims suffer.

### 2.2 The study Credit Card Cyber Fraud Detection

A Systematic Review by Btoush et al. (2023) highlighted that machine learning and data mining techniques have been employed more for credit card cyber fraud detection. They found that fraud detection systems are helpful because card transactions produce a lot of information, and it is hard to manually detect fraud. However, fraudsters

are constantly changing their approach which can make it hard for models.

In this section, the researcher studied the Cyber Financial Crimes in India. Cyber Financial Crimes in India have on the rise since the advent of digital banking, mobile apps, internet banking and online payment systems. There is a National Cyber Crime Reporting Portal with a structured manner for the population to report on cybercrime including financial fraud and there is Cyber Safety information for citizens. It is evident thereby that cyber financial fraud has a large issue to be addressed institutionally and through publicizing it. Government data also lumped credit and debit card frauds in the broader categories of 'cyber frauds' and 'financial frauds'. The Ministry of Home Affairs has indicated that the National Crime Records Bureau maintains records pertaining to all types of crimes including the Cyber Fraud and the fraud of credit/debit cards under the relevant categories of crime. This shows that the card frauds are not limited to banking environment and are an integral part of the Indian cybercrime ecosystem.

### 2.3 Read about security in digital payments

Digital payment security research highlights the importance of strong security measures, awareness, and regulation to create a secure and reliable digital payment environment. Indeed, banking frauds should be detected and monitored in a systematic manner and the Reserve Bank of India has laid down guidelines for classification and reporting of banking frauds. The importance of these regulatory actions is to increase the responsibility of banks and protect customers from unauthorized transactions.

Payment fraud in India has been a recent topic of

discussion among institutions and we see the correlation that social engineering, Phishing, fake links and misuse of identity are increasingly being used in Payment fraud attacks in India. PwC (2025) drew attention to the need for sophisticated fraud prevention measures, as well as greater regulatory measures and ongoing consumer awareness. Especially in India, where digital payments have been on a steep rise and the digital financial literacy of consumers is low.

According to the Ministry of Finance, digital payment transactions have exceeded 18,000 crores in 2024–25, highlighting the scale of digital financial transactions in India. The more people, merchants and institutions that enter the digital payment landscape, the more the risks to security increase. Thus, it is important to ensure the security of digital payment to prevent loss of trust in cashless payments from the public.

## **2.4 Research Gap**

The current literature is informative on the nature of card fraud, cyber financial crimes and digital payment security. However, most of the research studies have either been conducted at the national level or on the technological methods to detect fraud, or on general cybercrime trends. There are a few studies which have specifically focused on the credit card and debit card fraud in particular, particularly in Madhya Pradesh.

Yet another significant area of research is the lack on consumer awareness and victim experience in semi-urban and rural areas. While numerous research papers are on fraud detection technologies, user perceptions of fraud risks, user reactions to fraud events, and the difficulties of reporting or

recovering from fraud are largely overlooked. This is significant as many times the non-knowledge of the situation is a big cause of successful card frauds. The present study tries to bridge this gap by an analysis of the nature and extent of credit and debit card fraud in Madhya Pradesh. It emphasizes on creating awareness among users, fraud patterns, problems in the banking system and regulatory authorities, and the need for preventive measures. The study can thus be a useful addition to the literature in terms of regional perspective as well as analytical perspective on card fraud in the digital era.

## **3. The problem statement**

India's financial landscape has undergone a radical change with the swift growth in digital banking and electronic payment systems. Consumer credit and debit cards have become important enablers of cash-less transactions, offering convenience, speed and accessibility to the consumer. With the growing presence of Internet services, smartphones and digital commerce, card-based payment systems are being even more rapidly adopted. In tandem with these technological developments, there has also been an uptick in credit and debit card fraud, posing a major challenge for consumers, financial institutions, and regulatory bodies like the Reserve Bank of India (RBI, 2024).

### **3.1.1 Nature of Credit Card Fraud in Madhya Pradesh**

The digital financial transactions have been growing in Madhya Pradesh, owing to the increasing banking penetration, the government's efforts towards encouraging digital transactions, and the availability of internet. With more people

than ever before using credit and debit cards to pay for goods and services, make financial transactions and pay bills online, the opportunities for fraudulent practices have also been increasing. Card-related crimes such as phishing, card skimming, ID theft, fake customer care scams, unauthorized online transactions, data breaches, etc. have emerged as huge threats to consumers and financial institutions (Interpol, 2023).

Though there are increasing studies on digital payment, there is a lack of studies with respect to the extent, trends and nature of credit and debit card fraud in Madhya Pradesh. The true extent of the problem and the development of specific preventive measures is difficult because detailed empirical studies are lacking. Therefore, it is important to conduct an in-depth study of the cases of card fraud in the state to capture the increase of cases and factors associated with the risk of card fraud (United Nations Office on Drugs and Crime [UNODC], 2023).

### **3.2 Lack of Awareness**

One of the biggest reasons consumers could find themselves victim to card-related fraud is that they lack awareness of the cybersecurity practices and fraud prevention measures. Many users don't know the common phishing techniques used by cybercriminals, including fake e-mail messages, fake links, fake mobile applications, social engineering and requests for banking information. This implies that consumers might accidentally reveal personal information like card numbers, PIN numbers, OTP numbers, internet banking credentials, etc. (Kumar & Gupta, 2023).

This is particularly applicable in the zones of

divergence in terms of digital literacy across different groups of people. Digital Financial Services (DFS) have experienced a tremendous rise and have enabled a large population of customers to enter the digital economy for the first time in Madhya Pradesh. But, due to lack of awareness of safe ways to transact, they may be more susceptible to fraud. So, consumer awareness and awareness gaps of digital financial literacy are very important to reduce card fraud (World Bank, 2022).

### **3.2 Challenges for Banks and regulation bodies**

Banks and regulators are key to safeguarding the security and reliability of digital payment systems. The fraudulent activity in the cyber world, however, is constantly changing, making it difficult to detect, stop and respond to fraud. Cybercriminals often make use of advanced methods that involve exploiting technological weaknesses and people's mistakes to make fraud more difficult to detect (Association of Certified Fraud Examiners [ACFE], 2024).

Financial institutions incur costs associated with the resources required for building up security infrastructure, fraud detection, customer awareness initiatives, incident response, etc. Meanwhile, the regulatory bodies must develop effective policies, boost consumer protection regimes and uphold security standards. Nevertheless, barriers like the time lag in reporting frauds, cross-border cybercrime, technological limitations, and consumer awareness still exist in the effective prevention and control of frauds (RBI, 2024).

Therefore, the present study seeks to find the nature and extent of credit and debit card frauds in Madhya Pradesh, the level of awareness amongst the

cardholders to address credit and debit card fraud and the issues faced by banks and regulatory authorities in combating the fraudulent activities. The research's goal is to provide insights that could help policymakers, financial institutions and consumers create better strategies to ensure the security of digital payment systems.

#### 4. The purpose of the study

The present study is an effort to discuss about the increasing issue of Credit card and Debit card fraud in the context of increasing transactions in digital financial world in Madhya Pradesh. The study aims are listed below:

- (1) To analyse the occurrence of credit card and debit card theft in Madhya Pradesh.
- (2) To develop an awareness of most common fraud methods and fraud cards.
- (3) To study the reasons of card fraud.
- (4) To check the awareness level of the card users on fraud prevention.
- (5) Evaluate the effectiveness of the security measure adopted by banks.
- (6) To make suggestions as to the best ways of reducing card fraud.

#### 5. Research Questions

Based on the literature review of the current study, the following research questions serve as a guide:

- (1) Describe the various forms of card fraud in Madhya Pradesh.
- (2) What can be vulnerabilities and can they be increased?
- (3) Consumers' awareness of preventive measures.
- (4) Is the existing banking security system

sufficient?

The study aims to evaluate the effectiveness of the existing banking security measures to prevent fraud and safeguard consumers from unauthorized transactions and cyber risks.

#### 6. Hypotheses for the study

A null hypothesis for statistical analysis and an empirical investigation has been stated as follows:

**H<sub>0</sub>:** There is a relationship between consumer awareness, urban or rural area, banking security measures and the occurrence and prevention of credit/debit card fraud.

#### Alternative Hypothesis

**H<sub>1</sub>:** Consumer awareness, place of residence (urban/rural) and banking security measures are significantly related with occurrence and prevention of credit and debit card fraud.

#### 7. Research Methodology

Research methodology is the structured way that researcher collects, analyzes and interprets the data to achieve the object of research. It provides a scientific framework, making the scientific findings reliable, valid and accurate. The present study, "Credit and Debit Card Fraud in the Digital Era: An Analytical Study with Special Reference to Madhya Pradesh" is a secondary study and employs descriptive and analytical technique for discussing various aspects of card fraud.

##### 7.1 Research Design

This study is a descriptive and analytical type of research.

##### 7.1.1 Descriptive Research Design

Descriptive research deals with the description of the characteristics, nature and the actual situation of

a phenomenon. In this study descriptive approach is used to find out the current scenario of credit card and debit card and kind of frauds committed, consumer awareness and security measures taken by financial institutions. Descriptive design can be used to understand the trend and pattern of card related frauds in Madhya Pradesh (Kothari, 2004).

Descriptive approach is suitable for the study because the study does not intend to change any variable, but it only wants to get the factual data of the phenomenon of digital payment system, frequency of using the card, frauds cases, and the cybersecurity threat. It assists the researcher to arrange and record the information he/she has obtained from the various secondary sources systematically.

### **7.1.2 Analytical Research Design**

The study is an analytical type of research, and the causes, relationship and implication of credit card and debit card fraud was analyzed. Analytical approach involves the review of the existing data, reports and related studies of factors of fraud, effectiveness of fraud prevention and awareness and banking security systems for reducing fraud incidents.

The study employs analytical approach to attempt to draw some valid conclusions concerning the increased threat of digital payment methods and to make appropriate recommendations for the improvement of fraud prevention and consumer protection. Analytical research is especially beneficial for reading the information that is present and can provide insights that can help policymakers, financial institutions and regulatory bodies solve the issue more effectively (Sekaran &

Bougie, 2019).

### **7.2 Nature of Data**

The present study has been based on secondary data. Secondary data are data that have been gathered, compiled and published by other organizations, institutions, government agencies, researchers and financial institutions for a project other than the one at hand. These data can provide valuable insights into historical trends, fraud statistics, regulatory developments, and cybersecurity issues with respect to digital payment systems.

This study is appropriate in using secondary data as it allows the researcher to gain access to a wide array of reliable and authentic information regarding credit/debit card fraud without doing a large-scale primary survey. In addition, secondary data could be used for comparative analysis or to determine trends or changes over time (Kothari, 2004).

The data collected are analyzed systematically to know the prevalence of card fraud, factors responsible for card fraud, consumer awareness about fraud prevention and effectiveness of existing security measures in banking sector.

### **7.3 Sources of Data**

The study is based on several secondary sources for the relevant information concerning credit and debit card fraud, digital payment system, cybersecurity, consumer protection etc.

#### **7.3.1 RBI Reports**

The Reserve Bank of India (RBI) publishes reports, publications, circulars, annual reports and statistical bulletins which are an important source of information for the study. These documents offer

valuable insights into the trends of digital payments, statistics on banking fraud, regulatory frameworks, cybersecurity measures, and consumer protection policies adopted by the Indian financial system (Reserve Bank of India, 2024).

### 7.3.2 NCRB Reports

The National Crime Records Bureau (NCRB) publishes data that is used to gain insights into cybercrime and financial fraud trends and patterns in India. NCRB reports have official statistics relevant to this study regarding cybercrime incidents, fraud-related offences, and emerging challenges in digital security (National Crime Records Bureau, 2023).

### 7.3.3 Government Publications

Various reports, policy documents, discussion papers and publications from government ministries and departments have been consulted. It contains information on different digital payment initiatives, cyber-security policies, financial inclusion programmes, consumer awareness programmes and interventions by regulators to prevent financial fraud in the digital space.

### 7.3.4 Research Journals

Important sources of academic literature for the study are national and international peer reviewed research journals. Research articles on credit card fraud, debit card fraud, cybercrime, digital payment security, fraud detection technologies and consumer behavior and cybersecurity awareness are studied and a theoretical and empirical grasp of the content is gained (Button & Cross, 2017).

### 7.3.5 Websites and annual reports for banks

Various information from official websites and annual reports of public sector banks, private sector

banks and financial institutions has been analysed to know the security measures, fraud prevention plans, customer awareness programmes, and technological advancements in digital banking services. The sources provide a realistic view on the approach banks are taking to prevent card fraud and cyber-attacks against their users.

These various secondary sources will help in having a holistic idea about the topic and will help in an analysis of the phenomenon of credit/debit card fraud in Madhya Pradesh in the backdrop of the digital financial ecosystem of India.

## 8. The study area

### 8.1 Madhya Pradesh: An overview

Madhya Pradesh is one of the largest geographically States of India and it is also called as "Heart of India". Due to the central location of the state in India, it plays a very prominent role in the economic, agricultural, industrial and social development of the country. After the creation of Chhattisgarh state from southeastern districts of Madhya Pradesh, the state has been reorganized in November 2000. The state's profile is one of cultural diversity and heritage, a large population, rapidly urbanizing, and a developing digital infrastructure. In recent years, the banking sector in Madhya Pradesh has undergone substantial developments in banking facilities, financial inclusion, and the use of electronic payment methods, making it a suitable region to explore credit and debit card fraud (Government of Madhya Pradesh, 2024).

### 8.2 Demographic Profile

As per Census of India (2011), Madhya Pradesh has an estimated population of 72.6 million, one of the

most populous States in India. New population estimates are showing that the state's population has continued to rise as a result of natural growth and urbanization. The State has an even distribution of its population between the rural and urban areas and also has a variety of linguistic groups and socio-economic classes (Office of the Registrar General & Census Commissioner, India, 2011).

Education and digital literacy in Madhya Pradesh have seen a remarkable improvement in literacy rates due to the initiatives and efforts taken by the government towards promoting the literacy rate in Madhya Pradesh. Bhopal, Indore, Gwalior, Jabalpur, Ujjain and Sagar are the significant economic and technological centres. Yet a substantial portion of population is still living in rural areas and the availability of digital infrastructure and financial literacy could greatly differ. Given this demographic diversity, Madhya Pradesh is a crucial area to analyse consumer awareness and vulnerability towards digital financial fraud.

### **8.3 Banking Infrastructure**

Madhya Pradesh's banking system has seen tremendous growth in the last 20 years. There is a network of public sector banks, private sector banks, regional rural banks, cooperative banks, small finance banks and payment banks in the state. The Government of India has taken several steps towards promoting financial inclusion, including the launch of Pradhan Mantri Jan Dhan Yojana (PMJDY), which aims to provide banking services to those who have not been accessing them.

The commercial banks have expanded their banking branches, automated teller machines (ATM),

Internet and mobile banking throughout the State. As banking services are broadly available, people use credit cards, debit cards, banking through Internet and other electronic banking tools. Along with the rise in financial accessibility thanks to banking infrastructure growth, there has been a corresponding rise in cyber risks and card frauds, particularly in the case of users with lacking digital awareness (Reserve Bank of India [RBI], 2024).

### **8.4 Digital Payment Ecosystem**

With the technological advancements and supportive government policies, the digital payment ecosystem has expanded rapidly in Madhya Pradesh. Consumers are increasingly adopting electronic payment methods such as credit cards, debit cards, Unified Payment Interface (UPI), mobile wallets and internet banking and QR code-based payments. Digital payment adoption has also been further helped and propelled by the rising number of e-commerce platforms, digital marketplaces, and online service providers.

Digital India and the encouragement of cashless payment have also encouraged people and institutions to move from cash-based payment system to electronic payment methods. National Payments Corporation of India (NPCI) has significantly contributed to the robust development of the digital payment ecosystem, with the introduction of innovations like UPI, Immediate Payment Service (IMPS), and RuPay card services (National Payments Corporation of India, 2024).

Likewise, in the rapidly evolving digital transactions, economic opportunities and financial inclusion are also generated. It's also brought with it the potential for cybercrime such as phishing

attacks and ID theft, as well as card skimming, social engineering scams, and unauthorized financial transactions. Therefore, it is crucial for financial institutions and regulatory agencies to prioritize the security of digital payment systems.

### **8.5 Internet penetration and financial inclusion**

Internet access is an important determinant which influences the adoption of digital finance. In the last ten years, Madhya Pradesh has witnessed significant growth in internet penetration and this has been supported by the development of telecommunications infrastructure, availability of low-cost smart phones and the growth of mobile network coverage. With the internet becoming more ubiquitous, more people are participating in online banking and using various digital payment apps and e-commerce platforms (Telecom Regulatory Authority of India [TRAI], 2024).

Financial inclusion programmes have also significantly contributed to the mainstreaming of citizens into the formal financial system. The increased access to banking and financial services in the rural areas, and among the economically weaker sections of people in the society has been facilitated through the initiatives such as PMJDY, Aadhaar enabled payment mechanisms, direct benefit transfers, digital literacy, etc. Consequently, millions more people in Madhya Pradesh are now making financial transactions digitally, instead of using cash-based systems only (World Bank 2022). But cybersecurity awareness, safe digital practices, and fraud prevention are still problematic. Education and digital literacy and tech familiarity are still different, which impacts consumers' ability to recognize and deter fraudulent activities.

Therefore, it is necessary that a socio-economic and technological approach is required to analyse the credit card fraud and debit card fraud in Madhya Pradesh, so as to comprehend the fast-changing financial digital environment and come up with effective measures to safeguard the consumers.

## **9. Analysis and Interpretation**

Analysis and interpretation of data is an important part of the research process as it makes it easier to examine the relationship among variables and helps in drawing meaningful conclusions from the collected data. The present chapter focuses on analysing socio-economic profile of the respondents, pattern of card usage, experience with card fraud, awareness of security measures and perceptions of Banking security measures. Results are discussed in light of purpose of the study and problem of credit/debit card fraud in Madhya Pradesh.

### **9.1 Characterisation of the socio-economic background of the victims**

This socio-economic profile of the victims gives an understanding of the demographic and economic characteristics of the study victims. These features have an impact on the behaviour of digital payments, the awareness of digital payments and the vulnerability of digital payment fraud.

#### **9.1.1 Age of Victims**

Age is an important factor affecting the use and adoption of digital payment system. Youth tend to know more about technology and digital platforms while older users are likely to have more of a challenge when it comes to new payment methods. Analysing the age distribution can be used to understand the age groups that tend to use credit

and debit cards more and those that might be more susceptible to fraud because they lack technological knowledge (World Bank, 2022).

### 9.1.2 Gender

Gender-based analysis can be leveraged to understand any male/female specific trends with regard to card usage, fraud experience and awareness. Gender-specific awareness and security measures for consumers can be beneficial, as an analysis of gender characteristics can be helpful (Reserve Bank of India [RBI], 2024).

### 9.1.3 Education

Education is a crucial determinant in individuals' understanding of digital technology and cybersecurity. The more education one has, the more likely they will be to know what they are doing to protect themselves from fraud and to make transactions secure. Therefore, by conducting educational qualification analysis, the relationship between education and the vulnerability to card frauds can be analysed (Kumar & Gupta, 2023).

### 9.1.4 Occupation

The occupational position is used as an indicator of economic and technological exposure of the respondents. People who work in professional, business, service, and technology occupations might be more likely to make digital payments than others. Differences in transaction habits and awareness of financial security in digital transactions can be determined from the characteristics of the occupation.

### 9.1.5 Income Level

One of those factors is the income level that influences the use of credit and debit cards both in terms of frequency and amounts. High-income

earners may use their cards more frequently to pay for goods and services, invest and otherwise use the Internet, thus exposing themselves to a greater risk of card fraud. A look at income characteristics sheds light on income and how it relates to card use and vulnerability to fraud.

## 9.2 Card Usage Pattern

Given this depth of knowledge, it is crucial to recognize the trends of card use, which can offer insight into cardholder behavior and issues that can lead to card-related fraud.

### 9.2.1 The number of cards purchased

Depending your banking requirements and financial preferences, the respondents are allowed to use both debit cards as well as credit cards. Debit cards will be used more often for paying bills, drawing cash from the bank, credit cards for shopping online, travelling and instalment payments. Type of Card Used: Understanding this aspect of transactions can help identify patterns of usage and potential security vulnerabilities (RBI, 2024).

### 9.2.2 Frequency of Transactions

Respondents' use of cards, when they use them, indicates they are using electronic payment methods. There may be a greater number of transactions for frequent users, making them potentially more susceptible to cyber threats. The analysis of the frequency of transactions can indicate the degree of digital payment adoption by respondents and degree of association to fraud experienced.

### 9.2.3 Purpose of Usage

Different rates of card usage can be driven by consumer needs. These can involve things like online shopping, bill payments, travel, retailing,

educational and businesses transactions. Why a card is being used could be an indicator of a transaction that is more likely to be fraudulent and susceptible to cyber threats.

### 9.3 Incidence of Fraud

One of the most significant parts of the study is the incidence of fraud since it is directly related to the prevalence and magnitude of credit card and debit card fraud.

#### 9.3.1 Experience of Fraud

This section is an analysis of the respondents who suffered any sort of card fraud in the process of making use of the digital payment systems. This analysis of the proportion of respondents impacted by fraud can reveal the level of fraud in the study area, and insight into consumers' vulnerability (Association of Certified Fraud Examiners [ACFE], 2024).

#### 9.3.2 Fraud encountered

Respondents who have been hit by fraud may see a variety of fraudulent activities including phishing, card skimming, identity theft, unauthorized transactions, fake customer support calls, malware attacks and fraudulent links. The most prevalent frauds that consumers are facing can be identified by reviewing the type of frauds encountered and to develop more specific method of preventing the fraud (Interpol, 2023).

#### 9.3.3 Financial Loss Incurred

Fraud involving cards can result in loss of money for the cardholder. Financial losses that respondents reported in connection with their responses helps to gauge the economic impact of fraud activity. The size of the financial impact needs to be known as it is crucial to the assessment of the gravity of the

issue and the efficacy of current consumer protection measures.

### 9.4 Knowledge of Security Measures

Consumer awareness is an important part of the prevention of card related fraud. This section explores the respondents' cyber security and safe transactions knowledge.

#### 9.4.1 How OTP security works

As a second layer of authentication, we frequently come across One-Time Passwords (OTPs) in digital services. Respondents' knowledge about OTP security, such as not giving OTP to unauthorized persons is an indicator of their awareness about fraud prevention. By having the right OTP security knowledge, the chances of such unauthorized transactions can be significantly reduced (Reserve Bank of India, 2024).

#### 9.4.2 Awareness Phishing attacks

One of the most widespread ways that cybercriminals are getting sensitive financial information is through phishing. Assessing the respondents' awareness of phishing attacks can be useful to gauge their ability to identify phishing emails, messages, websites and phone calls designed to acquire personal information (United Nations Office on Drugs and Crime [UNODC], 2023).

#### 9.4.3 Safe and unsafe online transactions

Safe online transaction practices include using secure websites, regularly changing passwords, avoiding suspicious links, using two factor authentication and checking account activity. The findings on the awareness and use of such practices offer insights into how ready the respondents were to prevent digital financial fraud.

## 9.5 Evaluation Security Measures in Banking

Banks are essential in preventing consumers from falling prey to fraud by having technology, monitoring systems, and customer service employees.

### 9.5.1 Customer Satisfaction with Bank Safeguards

In this research, the respondent perception towards the effectiveness of security measures adopted by the banks was measured. Examples include EMV chip cards, transaction alerts, biometric authentication, fraud monitoring systems, secure payment gateways, and multi-factor authentication mechanisms, to name a few. This enhances the perception of customers and in turn increases their trust in security systems in banking.

### 9.5.2 Satisfaction grievance redressal mechanisms

Grievance redressal systems have to be effective to deal with fraud complaints and help victims to recover losses. It assesses customer satisfaction with banks' complaint processes, complaint timeframes, customer service and complaints and dispute handling. Satisfaction levels are higher, the better the institution is at managing issues related to fraud and protecting consumers' interests.

Based on the study and analysis conducted on these variables, an overall idea about the factors affecting credit card fraud and debit card fraud in Madhya Pradesh could be gathered. The findings lay the groundwork for testing the study hypotheses and make recommendations on how to make digital payments more secure and protected.

## 9.6 Hypothesis Testing

One of the important statistical techniques used to test whether the assumption made by the researcher is true or not is Hypothesis Testing.

**Basis of Testing:** For testing the relation between consumer's awareness, urban/rural, banking security measures, credit card fraud and credit/debit card fraud occurrence and prevention hypothesis testing is done in the present study. The goal is to determine the significance of these factors in determining who is vulnerable to card fraud in the electronic payments landscape.

The study was conducted based on the following hypothesis:

- **Null Hypothesis (H<sub>0</sub>):** There is no significance related to the consumer awareness and perception on residing area (Urban or Rural), banking security measures and credit/debit card fraud occurrence and prevention.
- **Alternative Hypothesis (H<sub>1</sub>):** Consumer awareness, place of residence (urban/rural), banking security measures and its relationship with the occurrence and prevention of credit/debit card fraud is significant.

The basis of testing is the hypothesis which is tested based on secondary data available through reports from the Reserve Bank of India (RBI), National Crime Records Bureau (NCRB), Government publications, Banking Reports and other previous studies related to digital payment security and financial fraud. The findings are derived from the patterns and relations observed in consumer awareness, geographical location, banking security practices and card fraud cases.

**Analysis and Interpretation:** Literature review and secondary data available indicated that consumer awareness is one of the significant factors to reduce credit and debit card fraud. Those who have knowledge about phishing attacks, OTP security, suspicious links, password security and safe online transaction practices are less prone to target of fraudulent practices. Several studies have removed lack of awareness as one of the most significant factors contributing to the successful cyber fraud and unauthorized card transactions (Kumar & Gupta, 2023).

It also reveals the gap that exists between the urban and rural consumers in terms of access to the digital infrastructure and their cybersecurity awareness. Overall, urban users are more likely to be exposed to digital technologies, internet banking and financial literacy programmes and therefore, are more likely to be aware of fraud prevention. However, some of these rural users may face issues with digital literacy, inadequate awareness campaigns, and limited understanding of cybersecurity measures, which makes them vulnerable to fraud (World Bank, 2022).

There is also good evidence that banking security measures make a significant contribution to the prevention of card-related fraud. Security measures like two-factor authentication, EMV chip technology, transaction alerts, biometric verification, fraud monitoring systems, and secure payment gateways contribute to minimizing unauthorized transactions and boosting consumer trust in digital payment systems. Financial institutions that are constantly investing in their cyber security infrastructure are more successful in

reducing fraud risks (Reserve Bank of India [RBI], 2024).

Overall, it appears that there is a significant correlation between consumer awareness, geographical location and banking security practices with credit and debit card fraud occurrence and consumer preventive measures. Such developments contribute to the security and reduce the risk of fraud for digital payment consumers.

**Decision:** Based on the results of the analysis of the data available and supporting literature, the null hypothesis ( $H_0$ ) is rejected and alternative hypothesis ( $H_1$ ) is accepted.

### Results

The results of the study indicate that there is a significant relationship between consumer awareness, place of residence (urban and rural), banking security measures and the occurrence and prevention of credit and debit card fraud.

The findings indicate that it is important to raise awareness among consumers, to have secure banking systems, and to increase consumer digital literacy, particularly in rural areas to fight credit and debit card fraud. The study emphasizes the need for financial institutions, regulators, government entities, and consumers to work together to create a secure and safe digital payments environment. Continual technological innovations in banking systems, along with regular cyber security training and enhanced awareness initiatives, can greatly reduce the incidence of card fraud and build confidence in online banking.

### 10. Findings of the Study

The findings of the study are presented below:

Findings of the study have been derived from the analysis of the secondary sources such as publications of Reserve Bank of India (RBI), National Crime Records Bureau (NCRB), various government publications, banking institutions, research journals and other sources. The study will provide insights into the occurrence of credit card fraud, debit card fraud, consumer awareness, security challenges and effectiveness of preventive measures in Madhya Pradesh and the Indian digital payment ecosystem, in general.

### 10.1 Using the data analysis the following major findings were derived

- (1) **Growing Credit/Debit cards frauds-** The study reveals that with the fast-evolving digital payment platforms and card-based transactions, the number of card-based frauds are also rapidly increasing. As credit and debit cards have become a popular way to pay for online purchases, cybercrime presents opportunities for criminals to exploit technology vulnerabilities and consumer carelessness in the era of digital banking and electronic payments. The Reserve Bank of India (RBI) has reported that financial frauds in India are still a major worry related to digital payment instruments (RBI, 2024).
- (2) According to the analysis, card fraud is a common application of new techniques such as phishing, fraudulent calls, fake customer care services, links and social engineering. There is a possibility that fraudsters could ask users to input their credit/debit card numbers, PINs, passwords or One-Time Passwords (OTPs). Human error and awareness are still key

aspects in successful frauds (Interpol, 2023).

- (3) **Consumer Awareness Significantly Influences Fraud Prevention-** One of the important findings of the study is that there is significant influence of consumer awareness in minimizing vulnerability to credit/debit card fraud. People who know safe online transactions, how to recognize a phishing, how to keep their OTPs secret and how to be safe online, are less likely to be subject to fraud. The higher the awareness, the better the safe behavior of digital payments and fraud prevention (Kumar & Gupta, 2023).
- (4) **Digital security awareness of urban consumers was higher than that of rural consumers-** Analysis revealed that generally, the digital security awareness of urban consumers is higher than the rural consumers. Urban users have greater awareness due to better access to technology, more education, more exposure to the internet, and more access to digital financial services. On the other hand, consumers in rural areas may be more susceptible to cybercrime because of digital illiteracy or lack of cybersecurity awareness (World Bank, 2022).
- (5) **Security measures at Bank help reduce fraud-** The study reveals that banks employ various security measures that are crucial in thwarting unauthorized transactions and financial fraud. Transaction alerts, EMV chip-enabled cards, biometric verification, and fraud monitoring systems and secure payment gateways improve transaction security and reduce the risk of card-related fraud. Financial

institutions have witnessed remarkable progress in identifying and curbing suspicious activities, largely due to the ongoing technological innovations (RBI, 2024).

(6) **Victims experience financial losses and psychological distress-** Card fraud can result in financial losses and psychological consequences, such as a loss of trust in e-payment methods, fear, anxiety and stress. It can be difficult for victims to recover funds and victims may not want to utilize digital financial services if they are victimized. It is not just the financial losses; the impact also extends to loss of trust by consumers in the digital economy (Button & Cross, 2017).

(7) **Awareness Programs and Digital Literacy are still insufficient-** According to the study, although banks and regulatory authorities are trying, there are still many consumers who do not have enough awareness to prevent cyber fraud. There is still a lot of ignorance among the users when it comes to getting to know the common fraud techniques and the recommended cybersecurity practices. This indicates a wider need to enhance financial education and raise awareness on different demographics about cybersecurity.

(8) **Fraud Prevention is a Multi-Stakeholder Endeavour-** The study reveals that credit and debit card fraud prevention is a "multi-stakeholder endeavour" encompassing a concerted effort from banks, regulators, government agencies, law enforcement agencies, technology providers and consumers. Consumer education, robust regulatory

systems, and timely reporting systems are needed in addition to technological solutions.

(9) **The challenges faced in Madhya Pradesh is also similar as the problems in the national digital payment system-** The results suggest that there is similarity between the problems of credit card and debit card fraud in Madhya Pradesh with the problems in the national digital payment system. The number of cyber-enabled financial crimes is likely to grow as the use of digital payments keeps growing in the state, if adequate measures are not taken to prevent such crimes. It is therefore important to have consumer awareness and cyber security infrastructure to have safe growth of digital financial services in the state.

(10) **Hypothesis Testing helps to reinforce the significance of awareness and security measures-** From the hypothesis testing conducted in the study, it can be seen that the factors of consumer awareness, place of residence (urban/rural) and banking security measure significantly affect the occurrence of credit and debit card fraud and the prevention of the same. The results support the alternative hypothesis and showed that these factors are crucial in determining vulnerabilities to fraud and the outcomes of fraud prevention activities.

Finally, the study can be concluded as Overall Finding that credit and debit card fraud has become a major problem in the digital age. While digital payment systems offer convenience and efficiency, consumer awareness, banking security measures, effective regulations, and ongoing cybersecurity education are all crucial to their effective and secure

use. Improvements in these aspects would make a huge impact in reducing fraud cases and have people more confident about the online financial exchange.

## 11. Conclusion

The financial services industry has undergone a digital revolution, which has had a massive impact on the way people and businesses transact. In today's payment environment, credit and debit cards are invaluable instruments of convenience, efficiency and accessibility. As dependence on digital payment systems has grown, so has the number of card-related frauds, creating significant problems for consumers, financial institutions and regulators.

The present study has made an attempt to highlight the issues of credit and debit card fraud in the digital era in particular in Madhya Pradesh. The secondary data analysis revealed that the increasing threats of card fraud are due to the rapid expansion of electronic banking, electronic commerce and online financial services. Phishing, card skimming, identity theft, unauthorised transactions and social engineering are still some of the fraudulent activities facing the security of digital payment systems.

One of the key findings in the study is that consumer awareness is a key element to fraud prevention. Those who have the education and understanding of what cyber security, OTP security, safe online practices, and fraud reporting are, are not as vulnerable to fraud. The findings also indicate that there are differences in awareness between each of the different demographic groups, in that, urban consumers have a higher awareness of

digital security than rural consumers.

The report also shows that the security measures implemented by banks are playing a significant role in minimizing the fraud risk. Electronic devices, such as EMV chip technology, two-factor authentication, fraud monitoring, biometric verification and transaction alerts all help to make transactions more secure. But the cybercrime gangsters are constantly updating their methods and security systems need to do the same.

The hypothesis testing carried out in the study substantiates the conclusion that both the consumer awareness and the place of living as well as banking security measures significantly affect the occurrence and prevention of credit and debit card fraud. Thus, to reduce fraud, technological responses are insufficient and the participation of consumers, regulatory cooperation and concerted institutional action are also required.

Last, the research highlights the role of digital payment systems in economic growth and financial inclusion and emphasizes the need to establish a safe, trusted and resilient digital financial environment for their continued prosperity. The awareness of cyber security, banking security and digital literacy in responsible practices are very important to curb credit and debit card fraud and ensure sustainable development of digital economy in Madhya Pradesh and the country in general.

## 12. Suggestions

- (1) Organize regular awareness campaigns for consumers on Credit/Debit card security.
- (2) Create awareness among users regarding Phishing, fake links, fake calls and OTP scam.

- (3) Expand financial education, especially of those who are not yet digital payment users, and those in rural areas.
- (4) Tell consumers to never pass on OTPs, PINs, passwords or card information to anyone.
- (5) Banks should develop more effective fraud detection mechanisms by using new Cyber Security technologies.
- (6) Use of multi-factor authentication and biometric verification should be endorsed for secure transactions.
- (7) Real time alert of transactions for all card activity.
- (8) Banks should keep customers informed on the latest cyber threats and measures.
- (9) The grievance redressal mechanisms for customers should be speedy, easy and effective.
- (10) Regulatory bodies need to enhance the monitoring and enforcement of the security standards of digital payments.
- (11) Improve collaboration with banks, cyber security agencies, law enforcement and technology providers.
- (12) This awareness in the field of cyber security should be created in the framework of school, college and professional education.
- (13) Consumers need to be aware of and advised to make online transactions with secure sites and trusted payment platforms.
- (14) Banks need to regularly audit their systems to discover and patch weaknesses.
- (15) There is a need to organise Digital safety campaigns at the State level to create

awareness and reduce card related frauds in Madhya Pradesh.

### 13. References

- Association of Certified Fraud Examiners. (2024). *Occupational fraud 2024: A report to the nations*. ACFE. <https://www.acfe.com>
- Basu, S. (2021). Cybercrime and digital financial fraud in India. *Indian Journal of Cyber Law*, 5(2), 45–61.
- Btoush, E. A. L. M., Zhou, X., Gururajan, R., Chan, K. C., Genrich, R., & Sankaran, P. (2023). A systematic review of literature on credit card cyber fraud detection using machine and deep learning. *PeerJ Computer Science*, 9, e1278.
- Button, M., & Cross, C. (2017). *Cyber frauds, scams and their victims*. Routledge.
- Census of India. (2011). *Primary census abstract: Madhya Pradesh*. Office of the Registrar General & Census Commissioner, India.
- Chandra, S., & Gupta, N. (2022). Consumer awareness and digital payment security in India. *Journal of Financial Services Research*, 14(3), 112–128.
- Das, A., & Roy, P. (2021). Cybersecurity challenges in digital banking. *International Journal of Banking and Finance*, 9(1), 78–94.
- Government of India. (2024). *Pradhan Mantri Jan Dhan Yojana: Progress report*. Ministry of Finance.
- Government of Madhya Pradesh. (2024). *Economic survey of Madhya Pradesh 2023–24*. Directorate of Economics and Statistics, Government of Madhya Pradesh.
- Interpol. (2023). *Global financial crime and cybercrime assessment report*. Interpol. <https://www.interpol.int>
- Jain, R., & Sharma, M. (2020). Digital payment adoption and fraud risks in India. *Asian Journal of Business Studies*, 11(4), 55–72.
- Kothari, C. R. (2004). *Research methodology: Methods and techniques* (2nd ed.). New Age International Publishers.
- Kumar, R., & Gupta, S. (2023). Cyber fraud and digital payment security in India: Challenges and preventive measures. *Journal of Banking and Financial Technology*, 7(2), 45–58.
- Malhotra, N. K., & Dash, S. (2019). *Marketing research: An applied orientation* (7th ed.). Pearson Education.
- Ministry of Electronics and Information Technology. (2023). *Annual report 2022–23*. Government of India.
- Ministry of Finance. (2024). *Digital payments ecosystem in India*. Government of India.
- Ministry of Finance. (2025). *Digital payment transactions surge with over 18,000 crore transactions in 2024–25*. Government of India.
- Ministry of Home Affairs. (2022). *Cyber fraud cases*. Government of India.
- National Crime Records Bureau. (2023). *Crime in India 2023*. Ministry of Home Affairs, Government of India.
- National Payments Corporation of India. (2024). *Annual report 2023–24*. NPCI. <https://www.npci.org.in>
- Office of the Registrar General & Census Commissioner, India. (2011). *Census of India 2011: Madhya Pradesh profile*. Government of India.
- Patel, K., & Singh, V. (2022). Online banking fraud and

- customer protection measures. *International Journal of Financial Studies*, 10(3), 88–101.
- PwC India. (2025). *Combating payments fraud in India's digital payments landscape*. PricewaterhouseCoopers.
- Reserve Bank of India. (2024). *Annual report 2023–24*. Reserve Bank of India. <https://www.rbi.org.in>
- Rogers, M. K. (2018). Identity theft and financial fraud in the digital age. *Journal of Financial Crime*, 25(1), 98–112.
- Sekaran, U., & Bougie, R. (2019). *Research methods for business: A skill-building approach* (8th ed.). Wiley.
- Sharma, A., & Verma, P. (2021). Consumer behavior towards digital payments in India. *International Journal of Commerce and Management Research*, 7(2), 34–42.
- Singh, P., & Sharma, A. (2022). Digital banking adoption and payment card security in India. *International Journal of Financial Studies*, 10(4), 89–102.
- Srinivasan, R. (2020). Cyber threats and digital payment security. *Indian Journal of Information Systems*, 12(1), 23–39.
- Telecom Regulatory Authority of India. (2024). *Indian telecom services performance indicators*. TRAI. <https://www.trai.gov.in>
- United Nations Office on Drugs and Crime. (2023). *Cybercrime and digital financial fraud: Global trends and challenges*. United Nations. <https://www.unodc.org>
- Verma, S., & Tiwari, R. (2022). Financial literacy and cyber fraud awareness among banking customers. *Journal of Emerging Technologies and Innovative Research*, 9(6), 210–220.
- Visa. (2023). *Global payment security report*. Visa Inc.
- World Bank. (2022). *Digital financial services and financial inclusion in India*. World Bank Publications. <https://www.worldbank.org>
- World Bank. (2022). *Digital financial services and financial inclusion in India*. World Bank Publications.
- World Economic Forum. (2023). *Global cybersecurity outlook 2023*. World Economic Forum.
- Yadav, S., & Mishra, A. (2021). Fraud detection mechanisms in digital payment systems. *International Journal of Computer Applications*, 174(15), 12–20.
- Zhou, X., Gururajan, R., & Chan, K. C. (2023). Machine learning approaches for credit card fraud detection: A systematic review. *PeerJ Computer Science*, 9, e1278.

\*\*\*\*\*