Asian And Pacific Economic Review
ISSN: 1000-6052

E-Rupee and Financial Cybercrimes: Exploring Technological Innovations and Regulatory Challenges

Kiran Pal Singh[1*], Dr. (Prof.) Jogiram Sharma[2]

[1*] Ph.D. Research Scholar, Dept. of Law, Geeta Global Law School, Geeta University, Panipat, Haryana.

[2] Guide cum Director, Dept. of Law, Geeta Global Law School, Geeta University, Panipat, Haryana.

DOI: https://doie.org/10.10399/APER.2025748350

Abstract

The study examines how technological advances affect legal concerns surrounding India's first digital money, the E-Rupee. This quantitative study will analyse how E-Rupee technological investment, cybersecurity measures, and regulatory stringency effect adoption rates and financial crimes. The complicated interactions of variables were examined using equation of structure modelling to determine the direct and indirect impacts of components. A substantial positive association between e-Rupee use and technological investment suggests that improved technology enhances adoption rates. More significantly, regulatory compliance and strong cybersecurity measures are essential to reducing E-Rupee financial criminality. When coupled with large technology expenditure, stricter laws boost adoption by creating a complementary strategy that links excellent rules to quality technology investments. This study may help policymakers and stakeholders promote safe and broad E-Rupee adoption as a digital currency.

Keywords: E-Rupee, Digital Currency, Financial Cybercrime, Technological Innovation, Regulatory Stringency, Finance Technological Innovations.

Introduction

The rapid digitization of financial systems has brought many improvements in monetary transactions, and CBDCs have emerged as the latest transformative innovation in this regard. Among these, India's e-rupee is a pioneering initiative that looks forward to changing the monetary landscape. The Indian government promoted fiscal inclusivity and modernized frugality by introducing digital payments- Cashless India in 2016, Unified Payments Interface, and the Public Payments Corporation of India, also known as NPCI. This was to ensure that there would be more digital transactions while printing paper currency would decrease costs [1]. This further encouraged private fintech companies and traditional public sector banks to participate in this movement through growing competition and innovation. The Digital Rupee, also popularly called the e-Rupee or e-INR, is an electronic version of the Indian Rupee that the RBI released in the last month of 2022. This is just the digital version of the paper currency, and therefore, it is regulated by the RBI, using distributed-tally blockchain technology. Intermediaries like banks offer the Digital Rupee, which is accessible in the same denominations as coins and paper money [2]. Two performance versions of the Digital Rupee have been made available by the RBI: Digital Rupee for Retail (e ₹- R) for retail transactions and Digital Rupee for Wholesale (e ₹- W) for fiscal

institutions. The digital rupee enables cross-border fiscal deals and can be held by non-residents to secure new deals.

Financial cybercrime rises with digital payment systems and CBDCs. Cybercriminals use weaknesses in the digital system to commit fraud, identity theft, and data breaches. The e-rupee adds a new dimension to cyber dangers, requiring a proactive strategy to protect consumers and organizations. Digital currencies are inherently vulnerable to cyberattacks. Phishing, ransomware, and DDoS assaults threaten payment system integrity and dependability. Digital transactions' anonymity, although advantageous for privacy, might facilitate money laundering and terrorist funding [3]. E-rupee use may enhance hackers' attack surface. This digital money exchanges sensitive financial data as more individuals use it, presenting abuse potential. Real-time threat monitoring, multi-factor authentication, and end-to-end encryption are crucial to reduce these dangers. Financial cybercrime prevention requires public awareness and education. Many consumers lack fundamental cybersecurity knowledge, rendering them susceptible to fraud. The government and financial institutions must prioritize user education and technology improvements to establish a safe and robust digital financial environment.

Technological innovation is both a driver of digital currency adoption and a critical enabler of cybersecurity. Blockchain, cryptographic algorithms, and secure digital wallets are among the technologies underpinning the e-rupee, ensuring its robustness against cyber threats. These developments not only improve transaction security but also improve transparency and trust in the financial system. CBDC, e-rupee, is the safest, most efficient, and most transparent way to carry out cash transactions. It uses distributed ledger technology and blockchain to confirm and remove transaction risks. The digital Indian Rupee, or e-Rupee, promotes financial inclusion, payment systems, and monetary policy. Digitizing money connects the unbanked to the official financial system, empowering them. The RBI shall issue CBDCs. Some of the CBDC benefits promised include enhanced security, reduced cost of transactions, faster speed in transactions, and increased financial access [4]. CBDC design often uses smart contracts, DLT, digital identity systems, encryption, mobile wallets, and APIs. CBDC design needs objectives, technology, and regulation. The proposed system would have a Private Blockchain for the Reserve Bank, authorized financial institutions, and a client consortium blockchain, account holders, companies, and licensed banks. Private blockchains provide privacy, governance, flexibility, scalability, and compliance advantages over public ones. Consortium blockchains are flexible and expandable owing to lower computer capacity, whereas private blockchains are more private. CBDCs may be created using blockchain and DLT technologies for secure and decentralized transaction records. They suit India's third-party apps and regulated banks. CBDCs are safer, more dependable, and more usable than fiat currencies, with better security, lower transaction costs, quicker transactions, and broader financial inclusion.

The Indian Digital Public Infrastructure (DPI) has promoted digital technologies and decreased digital divides. Blockchain-based Central Bank Digital Currency (CBDC) has assisted the financial revolution. This technology might change banking, finance, and payments. CBDCs employ private blockchains and public (permissionless) cryptocurrencies. Blockchain technology has changed central banks, commercial banks, IPOs, stock exchanges, and financial inclusion. Due to visibility, openness, trust, and automated transaction execution, rural Indians may access global markets [5]. The RBI has digitalised financial transactions and Fintech products such as UPI, AA, e-KYC, cash flow-based financing, e-agreement-mandate, and credit bureaus. Central Bank Digital Currency (CBDC), Public Technology Platform (PTP), Bharat Bill Payment System, Kisan

Credit Cards (KCCS), Digital Dairy loan distribution, UPI One World, and e-payment systems are some of the ways that RBI's CBDC infrastructure promotes innovation in the financial industry.

Blockchain technology stores every transaction in a distributed, tamper-proof ledger. Transparency eliminates fraud and ensures system accountability. Advanced cryptography also secures user data. Secure digital wallets with biometric identification and digitization improve user protection. Strong cybersecurity frameworks also depend on AI and ML [6]. These technologies help organizations quickly identify and react to risks by monitoring and detecting deficiencies. AI-based fraud detection solutions, for instance, could recognize suspicious transaction patterns to help curb financial losses. Technological progress alone will not suffice. Cybersecurity demands modern technology, governmental supervision, user education, and international cooperation. India can protect the release and adoption of the e-rupee while eliminating cybercrime risks through strategic technological applications.

Digital money issued by central banks is among the most important issues that carry many legal and institutional challenges toward their implementation. Central banks require capacity building and resource strength for currency reforms because CBDC's legal framework requires regulation. The changeover from physical currency to virtual one is difficult because of the ineffective supervision of CBDC. This would be a trust-based mechanism, and the central banks must be ready to consider risk management practices, governance, and internal arrangements [7]. The regulatory issues will have a strong legal framework for building the infrastructure. This needs interoperability with the existing payment system as well. Then comes dealing with cross-border transactions; for integration approach coordination, it would be needed among nations and with various institutions. To sustain long-term, the policymakers have to be agile and ready for the future. Building public confidence will require openness, sound cyber security, and effective resolution of concerns. The e-rupee revolutionizes digital financial inclusion and economic modernization in India. Its deployment must overcome several obstacles, from financial crimes to regulatory complexity. Technological innovation may improve security and usability, but legal, technological, and user-centric initiatives are needed. If India addresses these issues, it may assure the e-rupee's acceptance and create a worldwide standard for digital currency integration into national economies. This will help other governments with comparable objectives create a more secure and respectful global financial environment.

While significant studies have thoroughly explored the intention to adopt digital payment systems through the lens of TAM or UTAUT, minimal research exists to reduce the apprehension related to financial cybercrimes as motivating factors for adopting CBDCs. Even the studies reveal that a country's suitability for effective exploitation of digital currencies is founded on its ability to attain user trust with respect to the technology and its underlying security.

This paper examines the technical and regulatory issues that go along with the e-rupee, which focuses more on the impact it has on the cybersecurity aspect of financial transactions. It is, therefore, important to properly understand all these risks to protect users' interests and the institutions involved, especially since the number of cyberattacks on digital payment systems is rising. In addition, the study examines the influence of pre-existing digital payment networks, like the Unified Payments Interface (UPI), on consumers' electronic rupee uptake, which requires stringent regulatory measures to minimize the chances of cyber hazards. Below are the research objectives:

1. To examine the connection between the amount of money invested in E-Rupee technology and the pace at which companies and people adopt it.
2. To assess the effect of cybersecurity measures implemented and regulatory stringency on the incidents of financial cybercrime related to the E-Rupee.
3. To investigate the combined influence of regulatory stringency and level of investment in E-Rupee technology on the E-Rupee adoption rate.

The paper explores how the relationship of technical innovation relates to regulatory problems in digital currencies. It, therefore, forms an addition to the growing literature on the issue. The organization of this essay is as follows: Section 2 covers the technical foundation and connection between e-Rupee and UPI. Section 3 describes data collection and technique. Section 4 presents the research results, and the discussion is conducted in Section 5. It ends with suggestions for safe and efficient CBDC deployment and insights into policy implications in the Section.

Literature Review and Hypotheses Development

E-rupee and Digital Currency Innovation

Central banks worldwide are considering digital currencies, especially the introduction of Central Bank Digital Currencies (CBDCs), to enhance financial transactions and boost efficiency. Among these innovations, the E-Rupee is a technological breakthrough designed to deliver a secure, efficient, and accessible payment option for individuals and businesses [8]. The e-rupee aims to allow faster transactions, reduce transaction costs, and provide a digital alternative to traditional currency-based methods. As a technology-based solution, the E-Rupee looks to seamlessly integrate with existing financial systems while addressing concerns related to cybercrime and security [9]. Its adoption heavily depends on integrating the E-Rupee into the financial framework, while technological advancement and regulatory supervision will stand the test and ensure its success. [10] Central Bank Digital Currency, which goes by the initials CBDC, refers to digital currency presently issued by most central banks; the development so far discussed touched on its adoption in countries like China, Uruguay and the Bahamas, among many others. They used statistical techniques for bivariate correlation to determine which nations had the strongest link with CBDCs. Countries around the Baltic Sea, such as Finland, Estonia, and Lithuania, are seen to be the best candidates to establish CBDCs. Brazil and Uruguay in South America exhibit promising outcomes.

The [11] In the Fintech age, the battle between digital and conventional currencies is examined. Both sides will likely use digital collaboration methods, according to a version of the evolutionary game model of digital currency invention. After introducing financial regulation, financial institutions will engage in coordination. Thus, the currency selection technique is more susceptible to changes in incentive return and cooperation costs. [12] The global central bank digital currency competition has shifted from conceptual to practical stages because of the evolution of money and the growth of internet technologies. They explored the role of service innovation in central bank digital currency innovation using four dimensions: concept, interface, organization, and technological innovation. It suggests that the development and implementation of the central bank In the future, digital money will be a major advancement in the payment industry.

Hypotheses

Level of Investment in E-Rupee Technology and Adoption Rate

The level of investment in E-Rupee technology plays a pivotal role in determining its adoption rate among individuals and businesses. Higher levels of investment in research, development, and infrastructure facilitate a smoother transition from traditional payment methods and encourage greater public trust and usage. Prior research has shown that the level of investment in underlying technological advancements greatly impacts the acceptance of digital currencies. [13] A digital representation of India's national currency, the Digital Rupee blends the advantages of traditional currency with advancements in digital technology, providing benefits such as financial inclusion, lower costs on transactions, higher transparency, and improved monetary policy tools. Its adoption might transform transactions in India, reduce dependency on cash, promote a cashless society, and, consequently, influence international trade and foreign exchange markets. They focused on the potential implications and mechanisms of operation that the Digital Rupee may have on the Indian economy. [14] A new kind of currency known as Central Bank Digital Currencies (CBDCs) has emerged due to the digitization of money. They looked at working papers, studies, and circulars from central banks and financial organizations to clear up the confusion and misunderstanding around CBDCs and the e-rupee. Using empirical, conceptual, and qualitative research, they examined how CBDCs affected domestic and global economies. They helped people, organizations, and regulatory bodies by offering support and more insight. Thus, the following theory is put forward:

H1*: There is a positive relationship between the level of investment in E-Rupee technology and the adoption rate of E-Rupee among individuals and businesses.*

Cybersecurity Measures and Financial Cybercrime Reduction

Implementing robust cybersecurity measures is crucial for safeguarding financial transactions conducted through E-Rupee. Strong regulatory frameworks and advanced security protocols can significantly mitigate financial cybercrime risks, such as hacking, fraud, and unauthorized access. Empirical research suggests that cybersecurity enhancements reduce the likelihood of security breaches, promoting a safer digital payment environment. [15] They highlighted the global need for a comprehensive response to cyber threats and the risks associated with increasing technology reliance. They categorized cybercrimes into five: persons, property, government, and denial of service attacks. They emphasized the importance of cybersecurity in protecting critical information infrastructure and reducing cybercrime risks. It also discussed various cybersecurity technologies and methods to prevent cyberattacks. [16] They analyzed global cybercrime trends from 2016-2023, calculating national levels and modelling combat mechanisms. They emphasized how the COVID-19 epidemic and digital transformation had led to an increase in cybercrime. Nations with high cybercrime rates (Slovenia, Iceland, Moldova, Georgia) and higher levels of cyber security (Greece, Belgium, France, Germany) are identified. They aimed to create a safe, open, and open cyberspace, protect the population from cyber threats, and enhance financial monitoring procedures. Consequently, the following hypothesis is posited:

H2: *Stronger cybersecurity measures and higher regulatory stringency are associated with a reduction in financial cybercrime incidents related to E-Rupee.*

Combined Influence of Investment and Regulatory Stringency on Adoption Rate

The synergistic effect of high regulatory stringency and substantial investment in E-Rupee technology creates a conducive environment for its adoption. When coupled with technological innovation, enhanced regulatory measures lead to a well-regulated and secure digital financial system that promotes broader acceptance and usage. [17] India is considering adopting the e-Rupee as part of its monetary system. They analyzed this transition's feasibility, benefits, and challenges, focusing on regulatory framework, financial inclusion, security, and traditional banking systems. The study will provide recommendations for policymakers, financial institutions, and the public, examining the economic and financial goals, strategic implementation, and potential impacts on financial stability and privacy. They contributed to the ongoing discourse on digital currency adoption in India. [18] The Reserve Bank of India is aggressively working to move India's economy away from cash and toward digital. India has around one billion cards and two billion prepaid instruments, and its digital payment environment is expanding quickly. One innovative retail payment system is the Unified Payment Interface (UPI). They used the PESTEL approach to identify innovations and analyze the payment facilitation sector in India. This combined approach ensures efficient transaction processing and minimizes the risk of cyber threats. Therefore, it is hypothesized that:

H3: *The combined influence of regulatory stringency and the level of investment in E-Rupee technology significantly enhances the adoption rate of E-Rupee.*

Research Methodology

Research Design

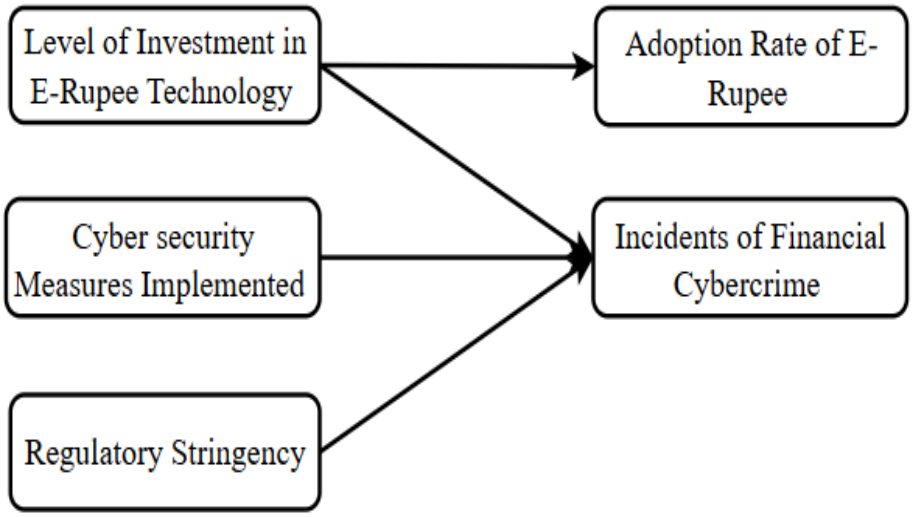
This research is being conducted in light of technological advancement and its relationship with the regulatory challenges related to the prevalence of financial cybercrime using a quantitative research design regarding e-rupee adoption. Understanding how investment in E-Rupee technology, regulatory stringency, and cybersecurity measures influence the rates of adoption as well as financial cybercrime. SEM using AMOS was applied because it was a model capable of simultaneously explaining relationships between many variables. It delves into the relationship between regulatory frameworks, technological advancement, and cybersecurity strategy to offer the government and other consumers concrete actionable recommendations for better use of E-Rupee as a secure digital currency.

Sampling

This study comprised 641 participants who were sampled purposively. The sample included people and organizations currently involved in digital financial transactions and had experience with e-rupee technology. Participants belonged to different demographic and professional groups, thus allowing a more inclusive study of perspectives about E-Rupee adoption and financial cybercrime. Inclusion criteria included people with prior experience with digital payment systems and cybersecurity issues. This helped the study to capture the apparent insights into the challenges and opportunities surrounding the implementation of the E-Rupee and its regulatory landscape.

Conceptual Model

The conceptual framework integrates five key variables: E-Rupee adoption rate, financial cybercrime incidents, investment in E-Rupee technology, cybersecurity measures, and regulatory stringency. This framework looks into relationships between these variables, focusing on how investment in technology and regulatory policies influence E-Rupee adoption while addressing and reducing financial cybercrime incidents. The model uses SEM and estimates these aspects' direct and indirect effects. It, therefore, provides an understanding of how those interplay in shaping the consumption of E-Rupee in a safe and regulated environment.



Data Collection Tools and Techniques

Data was gathered using a standardized questionnaire to get quantitative insights from the participants. The questionnaire validated scales on technological investment, regulatory stringency, cybersecurity measures, and their relationship with E-Rupee adoption and financial cybercrime. The online survey was used to facilitate widespread participation and ease of access. The data is analyzed using SEM-AMOS, which helps analyze complex interactions among variables. The analysis provided insight into the effectiveness of E-Rupee technology and regulatory frameworks in addressing financial cybercrime and promoting digital currency adoption.

Data Analysis

The gathered data would then be run through structural equation modelling (SEM) using the AMOS software to analyze them and allow an investigation of any proposed correlations among the variables being studied. Descriptive statistics were applied to collect key factors and participant demographics. SEM was applied to give insights into the direction and degree of the connections between E-Rupee use, cybersecurity measures, regulatory reliability, and technology investment. Model fit metrics were applied to test the conceptual framework's resilience. This approach

identified the elements impacting the E-Rupee's uptake and its function in financial cybercrime prevention.

Table 1 Sample characteristics

		Frequency	**Per cent**
Gender	Male	355	55.4
	Female	286	44.6
	Total	641	100.0
Age	18-30	276	43.1
	31-40	161	25.1
	41-50	106	16.5
	51-60	87	13.6
	Above 60	11	1.7
	Total	641	100.0
Annual Income	1-2 lakhs	126	19.7
	2-3 lakhs	238	37.1
	3-4 lakhs	199	31.0
	4-5 lakhs	41	6.4
	Above 5 lakhs	37	5.8
	Total	641	100.0

There were 641 individuals in the sample, with 44.6% female and 55.4% male. They were distributed according to age, with 43.1 percent being between the ages of 18 and 30, 25.1 percent being between the ages of 31 and 40, 16.5 percent being between the ages of 41 and 50, 13.6 percent being between the ages of 51 and 60, and 1.7 percent being beyond 60. Income per year: 19.7% made between 1-2 lakhs, 37.1% made between 2-3 lakhs, 31.0% made between 3-4 lakhs, 6.4% made between 4-5 lakhs, and 5.8% made beyond 5 lakhs. The demographic information indicates the diversity of the participants involved in the study, thus enabling a better understanding of the adoption of technology and financial cybercrime about E-Rupee.

Measurement objects.

Adoption Rate of E-Rupee

The e-rupee, India's first digital currency, is being adopted at a pace influenced by volume, merchant acceptance, integration into financial systems, registered users, and unbanked users. The e-Rupee is a medium of payment and legal tender, hence India's first digital currency. A standardized 6-item questionnaire with a five-point Likert scale was used to quantify ARE. "Strongly disagree" (1) to "strongly agree" (5) are the extremes of this scale. The measure captures various dimensions of E-Rupee adoption, including ease of use, preference over other digital payment methods, accessibility, transaction simplification, credibility, and future integration as a standard payment method.

Incidents of Financial Cybercrime

Financial cybercrime may, therefore, be defined as the theft of financial information or access to accounts through various means such as phishing, ransomware, identity theft, data breaches, online scams, extortion, loan fraud and cyberterrorism. All these risks threaten the integrity of financial systems, privacy, and security while affecting people, businesses, and the financial services sector.

Incidents of financial cybercrime were assessed using a six-item questionnaire on a five-point Likert scale. Participants indicated their level of agreement using a scale ranging from "strongly disagree" (1) to "strongly agree" (5). This scale assesses how people perceive the danger of cybercrime, how confident they are in security measures, how effective regulations are, and how confident they are in managing cyber threats related to E-Rupee transactions.

Level of Investment in E-Rupee Technology

This refers to the money allocated to create India's digital currency through investment in e-rupee technology. The electronic version of the Indian rupee is called the Digital Rupee or e-Rupee. The level of investment in E-rupee Technology was assessed through a 6-item scale using a Likert five-point scale. Answered items used a range between "Strongly disagree" received a score of 1, while "strongly agree" received a score of 5. It measures how the investment in E-Rupee technology improves functionality, visibility, user experience, satisfaction, and adoption.

Cybersecurity Measures Implemented

Cybersecurity measures protect against illegal use and unauthorized access to networks, devices, and data. Some examples include strong passwords, firewalls, antivirus programs, network security, application security, risk management, user education, incident management, monitoring, and frequent upgrades. All these will protect you from ransomware, malware, phishing schemes, data theft, and other online dangers. The cybersecurity measures implemented were evaluated using a five-point Likert scale with six items. From "strongly disagree" (1) to "strongly agree" (5), participants gave their ratings. This scale considers risk mitigation, frequent updates to security procedures, knowledge of security standards, and the strength of cybersecurity measures.

Regulatory Stringency

Regulatory stringency refers to the stringency of the laws, rules, or conditions governing a given area. Strong regulations are harsh and have a severe impact. To gauge regulatory stringency, a six-item survey on a five-point Likert scale was utilized. The range of responses was "strongly disagree" (1) and "strongly agree" (5). This measure captures participants' opinions on regulatory transparency, trust, deterrence of misuse, enforcement effectiveness, and adequacy of regulations to manage E-Rupee risks.

Constructs	*Measuring Indicators*	Source
Incidents of Financial Cybercrime	IFC1 1. I believe the risk of cybercrime is higher with E-Rupee transactions compared to traditional methods	Cybersecurity Reports and Whitepapers from Cybersecurity Firms (e.g., McAfee, Norton, Kaspersky): These reports discuss the frequency of financial cybercrimes and their implications.
	IFC2 2. News about cybercrime incidents makes me hesitant to use E-Rupee	
	IFC3 3. I feel confident in the security of the E-Rupee for financial transactions	

	IFC4 4. Regulatory actions effectively reduce financial cybercrime related to E-Rupee	• Kshetri, N. (2021). Cybersecurity and Financial Crime: A Global Perspective. Springer
	IFC5 5. Cybercrime incidents involving the E-Rupee are well-managed by authorities	
	IFC6 6. I trust that E-Rupee systems are equipped to handle potential cyber threats	
Cybersecurity Standards and Frameworks	CMI1 1. Cybersecurity measures implemented for E-Rupee are robust and effective	Government and Regulatory Guidelines: • National Cyber Security Policy, RBI's Cybersecurity Framework. • World Economic Forum (WEF) Report on Cybersecurity Measures for Digital Payment Systems. • Industry Whitepapers on Digital Payment Security: • Williams, P., & Johnson, D. (2021). Cybersecurity in Fintech: Protecting Digital Payments from Threats. Springer. • Cybersecurity Standards and Frameworks (e.g., NIST Cybersecurity Framework, ISO/IEC 27001)
	CMI2 2. I am aware of the security protocols protecting E-Rupee transactions	
	CMI3 3. Current cybersecurity measures reduce the risk of fraud in E-Rupee transactions	
	CMI4 4. I feel secure using the E-Rupee due to its cybersecurity measures	
	CMI5 5. E-Rupee's security measures are regularly updated to address new threats	
	CMI6 6. The level of cybersecurity in E-Rupee systems influences my decision to use it	

Level of Investment in E-Rupee Technology	LIET1 1. Investments in E-Rupee technology improve its functionality and reliability	Financial Reports of Digital Payment Platforms (e.g., Paytm, PhonePe, Google Pay): These often report on the level of investment in digital payment technologies. • Goyal, S. (2020). Investment in Digital Payment Technologies: A Strategic Approach to Financial Innovation. International Journal of Fintech and Financial Services. • Research Journals: • Bhat, M., & Kumar, R. (2022). Investment Patterns in Digital Payment Infrastructure. Journal of Financial Technologies
	LIET2 2. I am aware of recent developments in E-Rupee technology due to increased funding	
	LIET3 3. Technological advancements in the E-Rupee are visible and beneficial to users	
	LIET4 4. Increased funding for E-Rupee ensures better user experience and satisfaction.	
	LIET5 5. Investments in E-Rupee technology encourage broader adoption	
	LIET6 6. I believe there is sufficient investment to sustain the growth of E-Rupee technology	
Regulatory Stringency	RS1 1. The regulatory framework for the E-Rupee is transparent and user-friendly	Government and Regulatory Reports: • RBI's Regulatory Framework on Digital Payments and E-Rupee Initiatives. • Ministry of Finance, India - Reports on regulatory frameworks for digital payments. • Legal Journals and Articles:
	RS2 2. Stringent regulations enhance my trust in using the E-Rupee	
	RS3 3. I believe strict enforcement of regulations deters misuse of the E-Rupee	
	RS4 4. Regulatory bodies are effective in managing risks associated with E-Rupee	

	RS5 5. Compliance with E-Rupee regulations is essential for maintaining system integrity	• Singh, R., & Bansal, V. (2020). Regulatory Challenges and Financial Innovation: A Case Study of E-Rupee. International Journal of Financial Regulations
Adoption Rate of E-Rupee	ARE1 1. I find E-Rupee easy to use for everyday transactions.	Government Reports (e.g., Ministry of Finance, Reserve Bank of India (RBI)): These may provide official statistics and reports on the adoption rate of E-Rupee or other digital currencies. • Research Journals: • Sahoo, S., & Sahoo, S. (2021). Adoption of Digital Currencies: A Study on E-Rupee Adoption in India. Journal of Financial Technology and Regulation
	ARE2 2. I prefer E-Rupee over other digital payment methods.	
	ARE3 3. E-Rupee is accessible to people from all backgrounds	
	ARE4 4. Using the E-Rupee has simplified my financial transactions	
	ARE5 5. The widespread use of the E-Rupee enhances its credibility.	

Result

Measurement Model Assessment

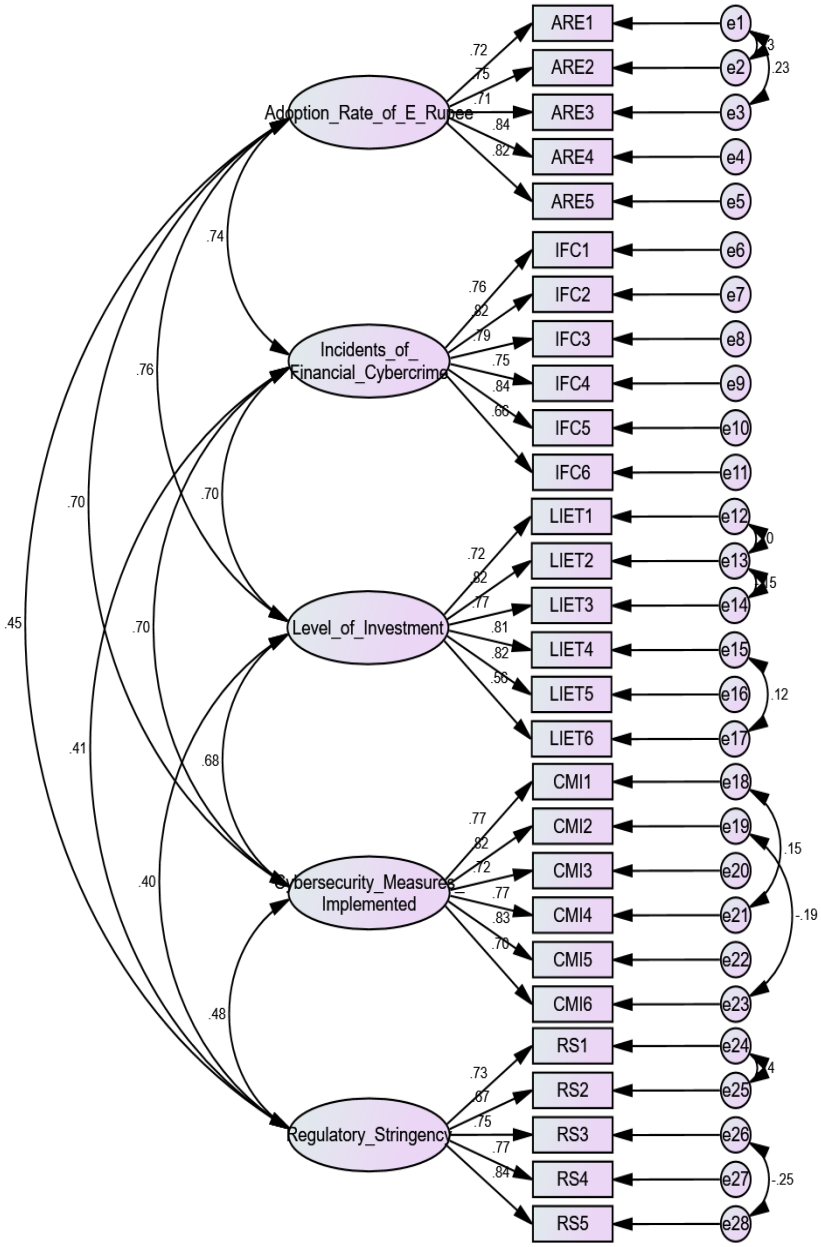


Table 2 Factor Loadings

	IFC	CMI	LIET	RS	ARE
IFC1	0.764				
IFC2	0.822				
IFC3	0.795				
IFC4	0.748				

IFC5	0.837				
IFC6	0.656				
CMI1		0.77			
CMI2		0.819			
CMI3		0.723			
CMI4		0.768			
CMI5		0.829			
CMI6		0.697			
LIET1			0.716		
LIET2			0.82		
LIET3			0.774		
LIET4			0.806		
LIET5			0.818		
LIET6			0.561		
RS1				0.728	
RS2				0.67	
RS3				0.749	
RS4				0.775	
RS5				0.842	
ARE1					0.717
ARE2					0.754
ARE3					0.707
ARE4					0.836
ARE5					0.823

The factor loadings for the several study-related variables are shown in the table. IFC (Investment in Financial Technology), CMI (Cybersecurity Measures Implementation), LIET (Level of Investment in E-Rupee Technology), RS (Regulatory Stringency), and ARE (Adoption Rate of E-Rupee) are the five parameters that the variables are categorized under.

With values ranging from 0.656 to 0.837, all of the IFC items show substantial factor loadings, suggesting a close connection between the factor and these indicators.

Strong loadings are also shown for CMI items, especially CMI2 (0.819) and CMI5 (0.829), indicating the importance of cybersecurity measures in the study's framework.

LIET's items have significant factor loadings; however, LIET6 has the lowest loading (0.561), suggesting a modest effect on the other items in this group.

Strong factor loadings are also shown in RS items, with RS5 (0.842) being the largest, indicating the impact of regulatory actions on the model.

All the ARE items show notable loadings, but ARE5 (0.823) has the greatest loading and strongly correlates with the E-Rupee adoption rate.

Although the intensity of these interactions varies considerably, the factor loadings generally indicate that all variables are suitably connected with their respective factors. The study shows strong signs for each component, which is essential for comprehending the connections in light of cybersecurity, technology adoption, and regulatory strictness.

Table 3 Construct validity and reliability

	Cronbach' s Alpha	**Composite Reliability (rho_a)**	**The Average Variance Extracted (AVE)**
Adoption Rate of E-Rupee	0.887	0.860	0.764
Incidents of Financial Cybercrime	0.894	0.863	0.770
Level of Investment in E-Rupee Technology	0.885	0.856	0.749
Cybersecurity Measures Implemented	0.895	0.862	0.767
Regulatory Stringency	0.866	0.855	0.752

The statistical methods used in this study to verify the construct validity and reliability of the variables are Cronbach's Alpha, Composite Reliability, and Average Variance Extracted (AVE), respectively. With a Cronbach's Alpha of 0.887, Composite Reliability of 0.860, and Average Variance Extracted (AVE) of 0.764, the Adoption Rate of the E-Rupee has high internal consistency. These results show that the approach is dependable and acceptable construct validity. As Cronbach's Alpha value is 0.894, Composite dependability value is 0.863, and AVE is 0.770, in the case of Incidents of Financial Cybercrime, the situation is highly dependent, similar to the previous scenario. These statistics reflect the consistency of the information along with concept validity. The Level of Investment in E-Rupee Technology is highly consistent, as indicated by its Cronbach's Alpha value of 0.885, Composite Reliability value of 0.856, and Average Variance Extracted (AVE) value of 0.749. The Cybersecurity Measures Implemented have high validity and reliability, with an Average Variance Estimator (AVE) of 0.767, a Composite Reliability Score of 0.862, and a Cronbach's Alpha Score of 0.895. The validity of this scale can be seen in the case of measuring Regulatory Stringency, given that it has excellent internal consistency expressed by Cronbach's Alpha of 0.866, Composite Reliability of 0.855, and Average Variance Extracted value of 0.752. All things considered, the results are such that all the variables come out trustworthy and valid, and this means that the measures utilized in the research are consistent and properly represent the constructs that were supposed to be measured.

Table 4 Discriminant validity

	Adoption Rate of E-Rupee	Incidents of Financial Cybercrime	Level of Investment in E-Rupee Technology	Cybersecurity Measures Implemented	Regulatory Stringency
Adoption Rate of E-Rupee	**0.874071**				
Incidents of Financial Cybercrime	.635**	**0.877496**			

Level of Investment in E-Rupee Technology	.642**	.631**	**0.865448**		
Cybersecurity Measures Implemented	.612**	.631**	.603**	**0.875785**	
Regulatory Stringency	.402**	.370**	.401**	.435**	**0.867179**

Each variable's Average Variance Extracted (AVE) square root is examined to determine its discriminant validity. This is achieved by ensuring that the values are greater than the correlations of the variables to be analyzed. The diagonal values in the table indicate all the square roots of the AVEs for every construction.

The adoption rate of the E-Rupee value is 0.874, which is higher than its correlation with other variables, such as Incidents of Financial Cybercrime (0.635), Level of Investment in E-Rupee Technology (0.642), and Cybersecurity Measures Implemented (0.612). This implies that it differs from the constructs since it is higher than the correlation with these other variables. Compared to the diagonal values in its correlations with other variables, Incidents of Financial Cybercrime (0.877) have a greater value, indicating its discriminant validity.

Since their diagonal values are greater than the off-diagonal correlations, the Level of Investment in E-Rupee Technology is 0.865, and the Cybersecurity Measures Implemented 0.875 show strong discriminant validity. Last but not least, the value of Regulatory Stringency (0.867) is greater than its correlations with the other variables, which supports the fact that it also retains discriminant validity.

The square roots of AVE, or all diagonal values, exceed the correlations between the variables, which indicates that the constructs are sufficiently dissimilar. This provides support for the discriminant validity, which is supported overall.

Structural Model Assessment

Table 5 Hypothesis Testing

	Path Coefficient	**β**	**p-Values**	**Results**
H1	LIET > ARE	0.712	0	Significant
H2	CMI, RS > IFC	0.105, 0.656	0	Significant
H3	RS,LIET >ARE	0.164, 0.633	0	Significant

It has been shown that there is a favourable correlation between the amount of money invested in the technology of E-Rupee and the rate at which people and companies adopt E-Rupee. (LIET is superior to ARE)

The results of Hypothesis 1 (H1) show that the Adoption Rate of E-Rupee (ARE) and the Level of Investment in E-Rupee Technology (LIET) are significantly positively correlated. Notably, the path coefficient for this relationship is 0.712, and the p-value for this hypothesis is 0. The fact that this is the case suggests that the rate of adoption of E-Rupee among people and enterprises is rapidly increasing in tandem with the growth in the amount of money invested in E-Rupee technology. Because the association is statistically significant, the hypothesis is supported.

It has been shown that a drop in the number of instances of financial cybercrime connected to the E-Rupee is correlated with the implementation of more stringent regulatory measures and more robust cybersecurity measures. (CMI, RS, and IFC are superior)

The second hypothesis (H2) questions whether a decrease in the number of incidents of financial cybercrime (IFC) is related to increased regulatory stringency (RS) and increased cybersecurity measures that have been implemented (CMI). The results of this study indicate that both RS (β = 0.656) and the CMI (β = 0.105) have statistically significant positive path coefficients with p-values of 0. This means that imposing stricter regulatory measures and implementing improved cybersecurity measures are significant factors that reduce the number of financial cybercrime events related to E-Rupee. Therefore, H2 is supported.

The overall impact of regulatory stringency and the degree of investment in e-rupee technology increases the rate of adoption of the e-rupee, as indicated in Hypothesis 3. (RS, LIET, and ARE are better).

Finally, Hypothesis 3 (H3) checks whether or not the combined effect of Regulatory Stringency (RS) and Level of Investment in E-Rupee Technology (LIET) increases the Adoption Rate of E-Rupee (ARE) by a significant margin. With a p-value of zero, path coefficients of RS (.164) and LIET (.633) are significant. This indicates that the adoption rate of E-Rupee is significantly and favourably affected by the confluence of strict regulations and investment in E-Rupee technology. This is shown by the p-value of 0. Further support is from H3 as well.

The data support all three hypotheses, with each relationship showing statistical significance and repeating the significance of technology investment, cybersecurity, and regulations. These items also impact the adoption of the E-Rupee and the decline of financial cybercrime.

Discussion

This investigation's findings agree with other research that has indicated the significant influence of technology investment and regulatory measures on the adoption of virtual money and the decrease in cybercrime in the banking sector. Research has shown that the higher the investment in digital payment technologies, the more people adopt them (Lee et al., 2019; Bada et al., 2020). According to the first hypothesis, there is a positive relationship between the adoption rate of the e-rupee and the money spent on its technology. The results of these past studies coincide with the current study. Such investments provide the infrastructure, security, and trust to encourage consumers and organizations to use digital currencies.

Since more robust cybersecurity and tighter regulations help reduce cybercrime risk, according to Yang et al. (2018) and Rajput et al. (2021), Hypothesis 2 seeks to test whether cybersecurity practices and regulatory severity influence financial cybercrime. As will be justified below, it is supported by both groups of researchers. It is shown by (Peltier et al., 2020) that previous studies focused on the important role of a strong cybersecurity model and transparent rule and regulation structure to instil confidence in an electronic financial structure, which ultimately reduces the propensity of crimes. Such opinion is echoed through the finding of this paper, which establishes

the requirement to protect the sanctity of an E-Rupee through appropriate regulatory approaches and cybersecurity methods.

Investigates the influence that regulatory stringency and investment in E-Rupee technology have on the adoption rate of E-Rupee. This one emphasizes the point that the combined variable increases the adoption rate. Such an ending supports Gupta and Arora's (2019) observation that legislative clarity and financial investment in digital technologies reinforce each other, fostering increased adoption of digital currencies. Zhang et al. (2020) concluded that a dual emphasis on building infrastructure with greater investment in technology and rigorous oversight of regulatory scrutiny results in a sharp acceleration in adopting new financial innovations. The effect that was achieved in this study combined with the results that Zhang et al. (2020) reached to their conclusion.
The results agree with previous studies, which illustrate the importance of technology investment, regulatory measures, and cybersecurity for the effective deployment and acceptance of digital currencies. This study contributes to the corpus of existing research by focusing on the E-Rupee and using actual data that seals the relationship between both.

Conclusion

The findings of this study highlight the main factors affecting E-Rupee adoption and the security level. The conclusions of this study further elucidate that investment level in E-Rupee technology and E-Rupee adoption are strongly positively correlated. The path coefficient for this relationship is 0.712 ($p = 0$), which means that higher technology investments correlate with higher adoption levels for individuals and businesses. It has also been demonstrated that the strictness of regulation and implementation of cybersecurity measures greatly influence the decrease in instances of financial cybercrime with regard to the E-Rupee. This is evidenced by the path coefficients at 0.105 and 0.656 ($p = 0$). Moreover, the cumulative effect of regulatory stringency and investment in E-Rupee technology significantly raises the adoption rate of E-Rupee, which is evident in the path coefficients at 0.164 and 0.633, respectively. This further proves that the adoption rate of the E-Rupee is rising heavily. This highlights that a comprehensive strategy that includes investment in technology and stringent regulatory measures is essential to ensure the safety of digital currencies such as the E-Rupee and their successful implementation.

Conflict of Interest Statement

The author has no conflict of interest with respect to the study, writing, and publication of this work. The views presented here are completely independent and meant only to add to the intellectual and professional conversation. The research has not been affected by any extraneous pecuniary, commercial, or personal interest. Furthermore, the author confirms that there are no competing interests that would compromise the view or analysis of the topic pertaining to E-Rupee, technological innovation, or financial cybercrime.

References

[1] Harshvardhan Govind, Aditi Nayan, and Priya Gupta, “The Evolution of Digital Payments: UPI, E-Rupee and the Future of Currency - in the Context of Urban Patna,” *Int. Res. J. Adv. Eng. Manag.*, vol. 2, no. 03, pp. 495–503, 2024, doi: 10.47392/irjaem.2024.0070.

[2] Ministry of Information and Broadcasting, “India – One of the pioneers in introducing CBDC,” pp. 1–7, 2022.

[3] S. Sehgal, M. Yasir, and S. Kour, “E-Rupee: Unlocking India’s Digital Economy, Challenges, and Opportunities,” *South Asian J. Soc. Stud. Econ.*, vol. 21, no. 8, pp. 1–13, 2024, doi: 10.9734/sajsse/2024/v21i8860.

[4] S. Jain, “Central bank digital currency – disruptive or need of the hour with special focus on indian e-rupee,” no. August, 2024.

[5] M. K. M., P. S. Aithal, and S. K. R. S., “Impact of Centralized Blockchain Digital Currency (CBDC): For Financial Inclusion and Sustainability,” *Int. J. Manag. Technol. Soc. Sci.*, vol. 9, no. 2, pp. 156–172, 2024, doi: 10.47992/ijmts.2581.6012.0351.

[6] J. Mu and D. Liu, “ScienceDirect Application of Artificial Intelligence Technology in the Field of Digital Currency Security,” *Procedia Comput. Sci.*, vol. 243, pp. 458–464, 2024, doi: 10.1016/j.procs.2024.09.056.

[7] A. Niroula and R. P. Gajurel, “Challenges of Central Bank Digital Currency Implementation : A Review of Literature,” no. December, 2024, doi: 10.3126/jom.v7i1.73517.

[8] L. Mallesha and A. Hn, “India ’ s Digital Currency (e ₹): A Comprehensive Study on CBDC,” no. September, 2024.

[9] N. Yanagawa and H. Yamaoka, “Digital Innovation, Data Revolution and Central Bank Digital Currency,” *Bank Japan Work. Pap. Ser.*, pp. 1–20, 2019.

[10] S. L. N. Alonso, J. Jorge-Vazquez, and R. F. R. Forradellas, “Central banks digital currency: Detection of optimal countries for the implementation of a CBDC and the implication for payment industry open innovation,” *J. Open Innov. Technol. Mark. Complex.*, vol. 7, no. 1, pp. 1–23, 2021, doi: 10.3390/joitmc7010072.

[11] B. Lan, L. Zhuang, and Q. Zhou, “An evolutionary game analysis of digital currency innovation and regulatory coordination,” *Math. Biosci. Eng.*, vol. 20, no. 5, pp. 9018–9040, 2023, doi: 10.3934/mbe.2023396.

[12] Q. Xing and Y. Li, *Research on the Innovation Strategy of Central Bank ’ s Digital Currency Application Based on Four Dimensions of Service Innovation 2 Progress and Development of Central Bank Digital Currency 3 A Brief Analysis of the Current Status of Service Innovation* , no. Icncss 2024. Atlantis Press SARL, 2024. doi: 10.2991/978-2-38476-230-9.

[13] G. S. Komma, ““ Digital Rupee : Unraveling the Future of Money in,” vol. 10, no. 12, pp. 194–201, 2023.

[14] S. F. Joseph and J. Peter Leo Deepak, “A Study on CBDCS and e-Rupee with Special Reference to e-Yuan BT - Current Trends in Economics, Business and Sustainability,” J. Aloysius Edward, K. P. Jaheer Mukthar, E. R. Asis, and K. Sivasubramanian, Eds., Singapore: Springer Nature Singapore, 2023, pp. 239–247.

[15] K. Adeniyi Phillips, Ibraheem Ojelade, Esther Taiwo, Callistus Obunadike and Oloyede, “CYBER-SECURITY TACTICS IN MITIGATING CYBERCRIMES: A REVIEW AND PROPOSAL,” *Soil Fertil. Sci. Publ. Inc.*, no. October, p. . 111–35, 2023, doi:

10.5121/ijcis.2023.13201.

[16] A. Kuzior, I. Tiutiunyk, A. Zielińska, and R. Kelemen, "Cybersecurity and cybercrime: Current trends and threats," *J. Int. Stud.*, vol. 17, no. 2, pp. 220–239, 2024, doi: 10.14254/2071-8330.2024/17-2/12.

[17] "Digital Currency Transition in India : Prospects , Difficulties and Consequences," pp. 1–50, 2024.

[18] C. Singh, "India's Success with the Digital Payment System," *Manag. J. Adv. Res. ISSN*, no. 6, pp. 32–38, 2022, doi: 10.54741/mjar.2.6.6.