WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Analysing User Trust and Cybersecurity Challenges in India's Cryptocurrency Ecosystem

Arpit Anand[1], Dr. M.S. Suganthiya[2]

[1]Student, Amity Business School, Amity University Maharashtra, Arpit.anand@s.amity.edu
[2]Assistant Professor, Amity Business School, Amity University Maharashtra mssuganthiya@mum.amity.edu

ABSTRACT

Cryptocurrencies and blockchain technology are reshaping how people handle money, and they are transforming the way money and investments are managed. With more people embracing digital assets, the websites individuals use to purchase, sell, and store these assets, such as cryptocurrency exchanges and wallets, are increasingly exposed to cybersecurity threats. This research aims to explore the risks associated with cryptocurrency, particularly in the Indian context, where its adoption is increasing rapidly but awareness of online security is generally low.

In 2024, a CoinSwitch report revealed that the lion's share of India's crypto investments were from only three large metro regions: Delhi-NCR (20.9%), Bengaluru (9.6%), and Mumbai (6.5%). These cities contributed more than 36% to the nation's overall crypto activity, demonstrating the way city centers are leading this digital revolution.

By surveys, expert opinions, and real-world case studies, this study concluded that blockchain itself is safe but the accompanying systems, such as apps and internet wallets, are exposed to cyberattacks. Cybersecurity threats include phishing, hacking, insider attacks, and scams. Artificial Intelligence (AI) is increasingly being used to guard and hack crypto platforms. Users are relying on AI tools for extra security, but they are also concerned with more intelligent attacks utilising the same technology.

Keywords: *cryptocurrency, blockchain technology, cybersecurity, digital assets, cryptocurrency exchanges, wallet security, phishing and hacking, artificial intelligence (AI), cyber threats, regulatory ambiguity, crypto adoption, urban crypto investment, and digital finance security*

1.0 INTRODUCTION

India's fast-developing digital landscape has resulted in broad-based acceptance of cryptocurrency, placing the nation in the top global crypto markets. Cryptocurrencies, which find their basis in blockchain technology, have been promised to transform the financial world with decentralised, transparent, and secure solutions against traditional banking. The decentralised nature of cryptocurrencies provides advantages like autonomy and transparency. But it also provides windows for malicious actors to take advantage of system weaknesses, which further result in security breaches, fraud, and loss of assets.

India's crypto universe, with 560 million users and fast-growing platforms such as WazirX and CoinDCX, is dealing with serious cybersecurity threats. Its users are being threatened by phishing and malware, as well as more advanced attacks on exchanges and wallets. Even though artificial intelligence (AI) is being widely used to secure crypto platforms, cyber attackers are also using AI for malicious activities. These threats combined with India's ambiguous regulations makes it even more riskier for the users.

This research paper will look into the cybersecurity issues experienced by the Indian cryptocurrency environment with regards to user trust, security measures on the platforms, and the specific hurdles in the local cybersecurity infrastructure. Through an examination of the status quo of cybersecurity practices among Indian crypto users and an assessment of the efficacy of these measures, the paper intends to provide an in-depth overview of the threats in the environment. Moreover, the research will evaluate how new technologies, such as AI, shape the trust and security dynamics of crypto platforms and seek the wider implications for both regulators and users in India's crypto market.

2.0 LITERATURE REVIEW

Blockchain Security and Vulnerabilities (Conti et al., 2018):

Conti et al. (2018) highlighted that although blockchain technology is secure in itself because it is decentralised in nature and cryptographic protocols are involved, the platforms developed around it, like cryptocurrency exchanges and digital wallets, remain extremely vulnerable. Phishing, malware attacks, DDoS, and theft of private keys are common attacks, and therefore, these interfaces become prime targets for cybercriminals.

User Trust in Digital Financial Platforms (Gefen et al., 2003):

Gefen et al. (2003) examined why trust is instrumental in digital service adoption. According to them, consumers are more inclined to adopt what they view as secure, transparent, and trustworthy platforms. This model is applicable to the crypto space, where financial and technological threats are co-entwined.

Cybersecurity and Regulatory Ambiguity in India (Kumar & Purohit, 2022):

Kumar and Purohit (2022) tested the Indian crypto domain, tracing regulation uncertainty and patchy platform operations as top forces affecting confidence among users. They further state that poor cybersecurity standardisation discourages even more investor faith in crypto asset platforms.

Artificial Intelligence in Crypto Security (Nassiry, 2019):

Nassiry (2019) examined the two-sided impact of Artificial Intelligence on the cryptocurrency landscape. While AI improves security via real-time anomaly detection, biometric authentication, and behavioural analysis, it also equips attackers with sophisticated tools to compromise systems, underlining the necessity of ethical deployment of AI.

Cybersecurity Awareness Among Indian Crypto Users (Singh & Kaur, 2021):

Singh and Kaur (2021) discovered that although crypto adoption is increasing in India, there is low user awareness regarding digital safety. The majority of the users have inadequate knowledge of cybersecurity tools and best practices, thereby being more exposed to scams, phishing, and identity theft.

Legal Framework and Platform Accountability (Rani & Das, 2020):

Rani and Das (2020) pointed out the weaknesses of India's legal framework in dealing with cybercrime related to cryptocurrency. Without effective policy enforcement, crypto platforms tend to function without standardised security protocols, exposing users to systemic vulnerabilities.

Public Education and Trust-Building Measures (Sharma, 2021):

Sharma (2021) explained how public awareness campaigns and user education contribute significantly to improving cybersecurity. The research highlights the need to educate users on two-factor authentication, hardware wallets, and identifying scam signs to minimise vulnerability and maximise platform trust.

3.0 RESEARCH OBJECTIVES

- Study cybersecurity flaws in cryptocurrency platforms, such as exchanges, wallets, and applications.
- Assess the contribution of AI to security enhancement as well as facilitation of cyberattacks, together with user attitudes towards AI tools.
- Analyse how user trust influences cryptocurrency adoption in India, taking into account the security of platforms, reputation, and regulation.
- Study regulatory and infrastructural issues in India's crypto environment and propose possible enhancements.
- Study user awareness of cybersecurity threats and determine areas of knowledge gaps.
- Offer suggestions to strengthen cybersecurity, build trust, and bring a secure Indian cryptocurrency environment.

4.0 RESEARCH METHODOLOGY

4.1 Area of the Study

The research will concentrate on the Indian cryptocurrency community in contrast with the international cases to provide a comparative perspective. The research aims to comprehend user behaviour, platform readiness, and regulatory reactions in the Indian market.

4.2 Sample and Sampling Technique

The primary dataset includes 66 responses collected through structured questionnaires distributed to Indian cryptocurrency users. A purposive sampling technique was used to ensure participants had experience with exchanges and/or wallets. Additional insights from cybersecurity professionals, regulatory reports, and public domain data form the basis of secondary research.

4.3 Type of Study

This is a mixed-method study employing both qualitative and quantitative techniques. The quantitative aspect focuses on statistical interpretation of user responses, while the qualitative aspect draws on expert opinions and case study analysis.

4.4 Tools for Data Collection

Primary Tools:

- Structured questionnaire (covering demographics, security practices, AI perceptions, etc.)

Secondary Tools:

- Academic journal articles
- Technical audit reports from cybersecurity firms
- Case studies and industry analyses
- Regulatory publications

4.5 Statistical and Analytical Methods

- Descriptive Analysis: To assess user habits and general perceptions.
- Comparative Analysis: Evaluating security measures across different platforms (DeFi, centralised exchanges).
- Visual Representations: Pie charts, bar graphs, and tables will be used to clearly present the data.

5.0 SCOPE AND LIMITATIONS OF THE STUDY

5.1 Scope

1. **Geographical Focus:** The research will be based on the Indian cryptocurrency environment. It will also take into account the increasing use of digital money in urban areas such as Delhi-NCR, Bengaluru, and Mumbai, and the challenges unique to these areas.
2. **Cryptocurrency Platforms:** The study will investigate the different cryptocurrency platforms, including exchanges, wallets (both software and hardware), and other blockchain-related services. Attention will be drawn to identifying the vulnerabilities of security on these platforms, e.g., phishing, malware, and fraud.
3. **Technological Focus:** The research will evaluate the impact of emerging technologies, especially Artificial Intelligence (AI), in enhancing security mechanisms as well as facilitating cyberattacks in the cryptocurrency market. It will also analyse how these technologies affect user trust and platform security.
4. **User Awareness:** The study will investigate how aware Indian cryptocurrency users are of cybersecurity best practice and threats, including such things as two-factor authentication (2FA), private key management, and the threat of holding assets on exchanges.
5. **Regulatory Analysis:** The research will explore the existing regulatory environment of cryptocurrencies in India and how the lack of clarity in current frameworks affects the security practices and risks of the ecosystem.

5.2 Limitations

1. **Regulatory Ambiguity:** Lack of a formal regulatory mechanism for cryptocurrencies in India constrains the research to give exact views regarding cybersecurity matters of governance and policy-related concerns.
2. **Rapid Technological Change:** Due to the rapid development of both blockchain technology and cybersecurity threats, the research captures the present situation but does not reflect anticipated future evolutions or new threats.
3. **Accessibility of Data:** Availability of detailed security breach information or internal cybersecurity protocols utilised by cryptocurrency platforms is sometimes restricted. Most platforms might not release the complete status of security incidents publicly, which may restrict the level of analysis in terms of actual-world cyberattacks.

6.0 ANALYSIS AND INTERPRETATION

This analysis explores the user's trust on the various cryptocurrency wallets and exchanges and assesses their knowledge about cryptocurrency. We have taken responses from 66 users from various age groups and occupations. The study also helps us to know how the users perceive the integration of AI in preventing cybersecurity attacks and price prediction.

6.1 Graphical Representation and Interpretation of Data

6.1.1 Vulnerability due to Digitalisation

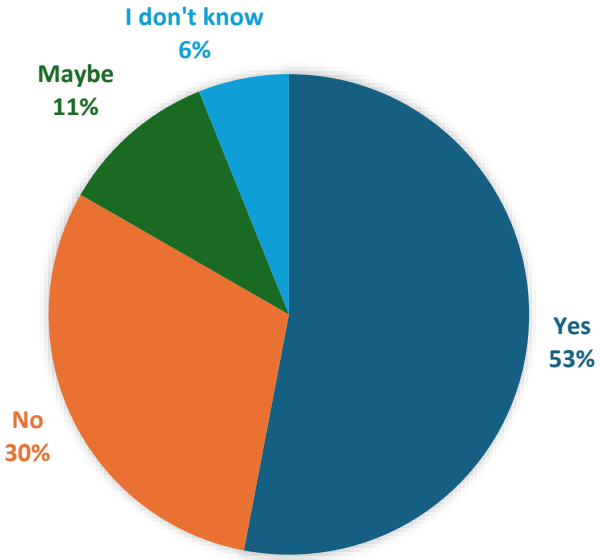

FIG. 3.1.(I) VULNERABILITY DUE TO DIGITALIZATION

Key Observations:

1. **Majority Perceive Risk**:

   Over half of the respondents (53%) believe that increasing digitalisation in the crypto ecosystem does increase vulnerability, indicating a strong perceived connection between technological progress and cybersecurity risk.

2. **A Significant Minority Feel Secure**:

   30% (20 people) feel no increased vulnerability, showing a notable portion of users remain confident in current systems — possibly due to better personal cybersecurity practices or reliance on trusted platforms.

3. **Uncertainty Exists**:

- 11% (Maybe) and 6% (Don’t know) reflect uncertainty or lack of knowledge, suggesting an information gap in how digitalisation impacts crypto security.
- This aligns with the finding that some users aren't fully aware of AI and digital threats despite using crypto platforms.

Interpretation- The responses suggest a growing concern among users regarding the risks posed by increasing digitalisation in cryptocurrency platforms. With over 50% acknowledging vulnerability, it's evident that while digital tools and AI offer improvements in security, they also raise the perceived exposure to cyber threats. This perception underlines the need for stronger risk communication, education, and transparent security frameworks within crypto platforms, especially as AI, automation, and digital assets become more integrated into the Indian financial ecosystem.

6.1.2 Concern about AI-powered attacks

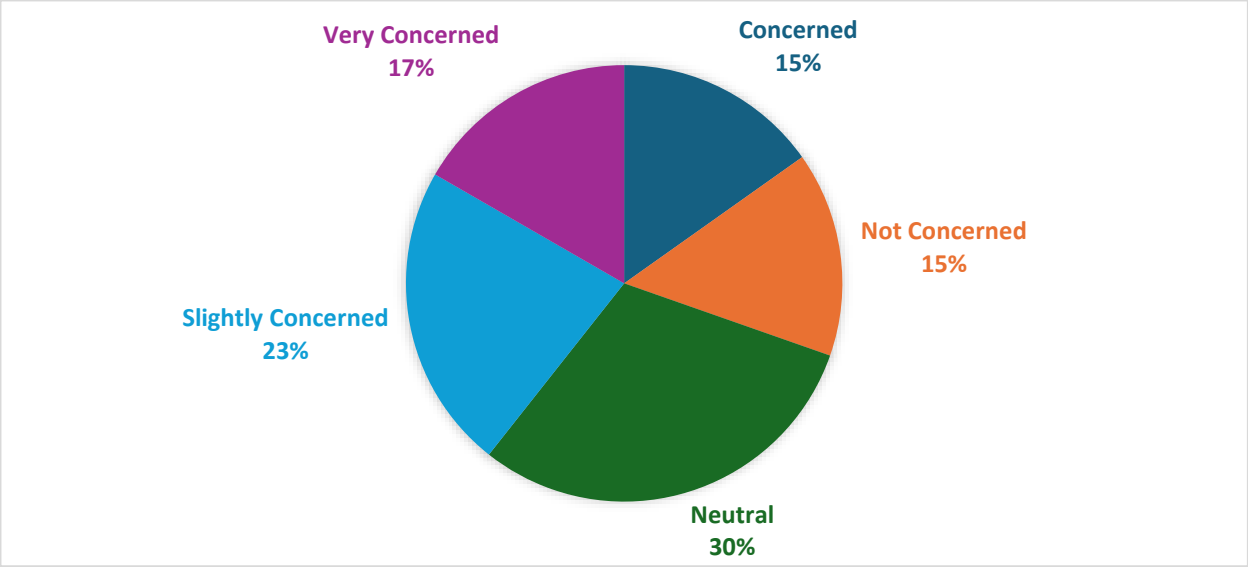

FIG. 3.2.(I) CONCERN ABOUT AI-POWERED ATTACKS

Key Observations:

1. **General Concern Exists (32%)**:

- Concerned and Very Concerned combined make up 32% of respondents (21 people).
- This reflects a growing awareness that AI, while powerful for defense, can also be weaponised for sophisticated cyberattacks, like deepfakes, automated phishing, or AI-based hacking.

2. **High Level of Uncertainty or Indifference (30%)**:

- The largest group is Neutral (20 respondents).
- This could indicate a lack of exposure or understanding of how AI can be used maliciously, which may be due to the relative newness of AI in the public discourse in India.

3. **Mild Concern in 23%**:

- These users are aware but not alarmed. They might recognize the threat but believe current systems or personal practices are enough to mitigate risks.

4. **Low Concern (15%)**:

- 10 users are not concerned at all, which may be due to:
- Limited usage of crypto
- Lack of awareness or belief in AI's capabilities

Interpretation- The data reveals a moderate but significant concern regarding AI-powered cyberattacks among Indian crypto users. Nearly one-third of respondents express high concern, highlighting a perceived dual-edge nature of AI in digital security. However, with 30% remaining neutral, it's clear that a sizable portion of users may lack full awareness of AI-related risks. This suggests a crucial need for greater education and transparency from crypto platforms regarding both the benefits and threats of AI integration.

6.1.3 Trust in AI-driven Security

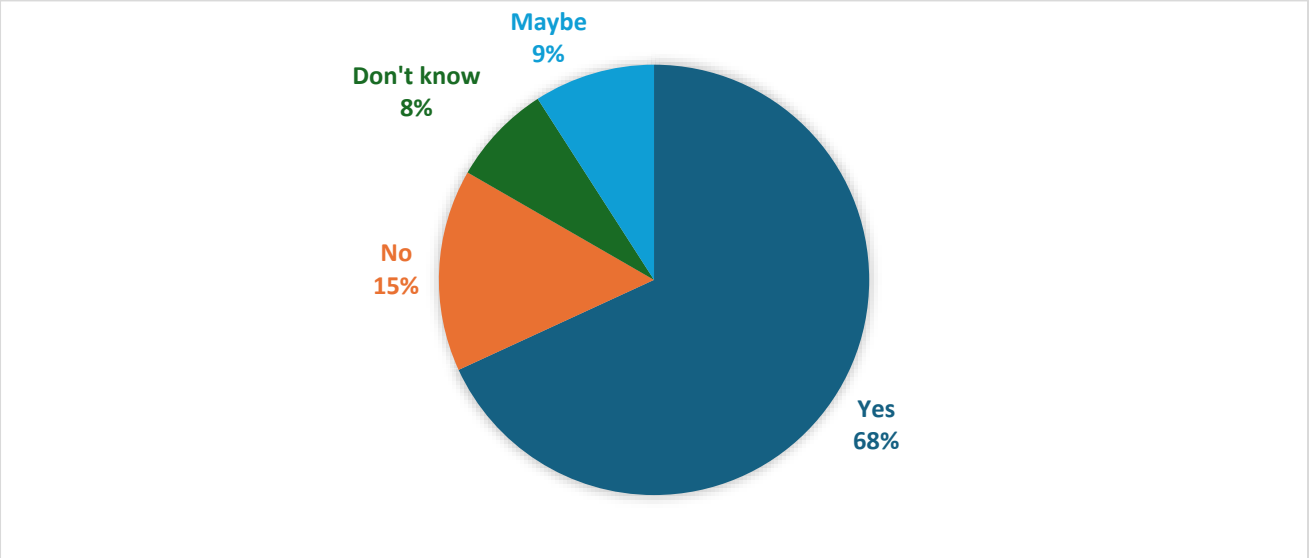

FIG. 3.3.(I) TRUST IN AI-DRIVEN SECURITY

Key Observations:

1. Strong Trust in AI (68%)

A significant majority of respondents (45 out of 66) express clear trust in AI-driven security features. This suggests growing acceptance of AI tools like:

- Biometric logins
- Behavior-based anomaly detection
- AI-authenticated transactions
- Real-time fraud alerts powered by machine learning

It also reflects increasing confidence in the automation of security protocols, especially given India's rapid digitalisation.

2. Limited Distrust (15%)

A smaller but notable group (10 respondents) does not trust AI-based security. This could stem from:

- Lack of transparency in how AI decisions are made
- Concerns about over-reliance on technology
- News coverage of AI-based privacy breaches or bias

3. Indecision/Uncertainty (17%)

The combined ‘Maybe’ and ‘Don’t know’ group represents 17%, suggesting:

- Users are open to the concept but need more information
- There's a lack of user education about how AI is currently applied in crypto security

Interpretation- The data reflects a generally positive attitude toward AI-driven cybersecurity solutions, with nearly 7 in 10 respondents expressing trust. This suggests a high potential for further integration of AI in safeguarding cryptocurrency platforms in India. However, the presence of uncertainty and scepticism among a small portion of users underscores the need for platforms to enhance transparency, provide clear documentation of AI functions, and educate users on the benefits, limits, and ethical use of AI in security.

This aligns with the broader hypothesis that while existing security frameworks show signs of user acceptance, further innovation and risk communication are necessary to mitigate evolving cyber threats, particularly those that AI could introduce or help defend against.

6.1.4 Effectiveness of Security Measures

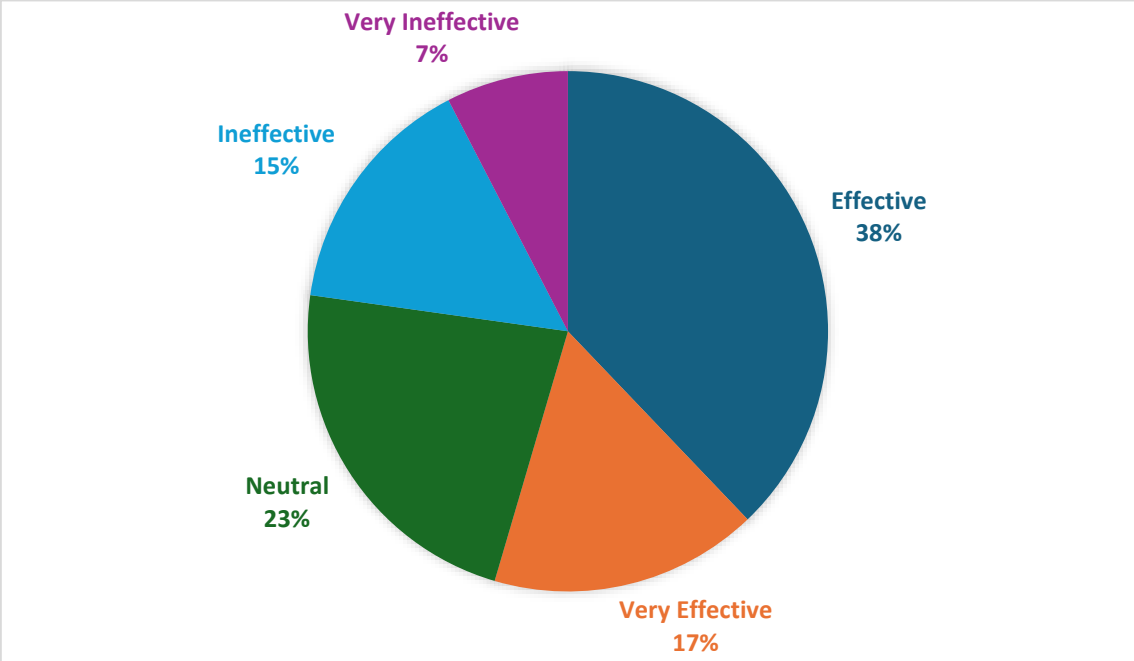

FIG. 3.4.(I) EFFECTIVENESS OF SECURITY MEASURES

Key Observations:

1. Majority Perceive Security as Effective (55%)

A combined 55% of respondents (25 effective + 11 very effective) believe that current security measures like 2FA, cold storage, encryption, etc., are performing well in safeguarding crypto assets. This suggests a general sense of confidence in current cybersecurity frameworks.

2. Moderate Skepticism or Uncertainty (23%)

The 23% neutral responses may reflect:

- Limited technical understanding of what qualifies as "effective" security
- No personal experience with cyber threats to judge effectiveness
- Trust in platforms but lack of deep insight into backend security practices

3. 23% Perceive Measures as Ineffective

(15% ineffective + 8% very ineffective) reflect a significant minority that doubts the sufficiency of current protections. This could relate to:

- Inadequate awareness campaigns by exchanges
- Concerns over rising AI-powered attacks
- Visibility of past global breaches despite personal safety

6.2 Descriptive Analysis

- **Cyber Attack Experience:**
    - **0 out of 66 respondents** have experienced a cyber attack directly — this heavily suggests that *at least in the current sample*, **existing cybersecurity measures are working effectively**.
- **Security Measure Usage:**
    - 75%+ of respondents use **2FA** and **strong passwords**.
    - Over 45% utilise **encryption** or **biometric authentication**, and about 38% use **cold storage**.
    - Most users rated security effectiveness as **4 (Effective)** or **5 (Very Effective)**.

- **Confidence in Exchanges:**
    - A majority **believe current security protocols are sufficient**.
    - However, **64% of users expressed willingness to accept higher fees** in return for **enhanced security measures** — showing openness to **improvement** even if current systems are doing their job.
- **AI & Digitalisation Impact:**
    - While 76% believe **AI can improve cybersecurity**, around 48% are **concerned** or **very concerned** about **AI-powered cyberattacks**.
    - 53% believe digitalisation could **increase vulnerability**, indicating a level of **future-oriented caution**.

6.0 CONCLUSION

The data analysis shows that although most users are confident in the current level of cybersecurity within cryptocurrency platforms, the majority are concerned, doubtful, or unsure. More than half of the participants (53%) feel that heightened digitalization makes them more vulnerable, showing high levels of concern for the changing cyber threat environment. Moreover, 32% of users show explicit concern about AI-based cyberattacks, and 30% show no opinion, indicating ignorance or lack of perception of the dangers of artificial intelligence in this field.

Notwithstanding these fears, faith in AI-based security is surprisingly strong, with 68% of interviewees showing confidence in such features as biometric authentication and real-time fraud alert. However, the combined 32% are either untrustworthy or unsure of AI in cybersecurity, which indicates a definite requirement for better transparency and user education. For users' perceptions of the effectiveness of existing security features, 55% consider them to be effective or very effective, with 46% either being neutral or unimpressed, reflecting mixed confidence in the protection provided by exchanges and wallets.

Most notably, none of the respondents reported being victimised by a cyberattack, and security tool penetration is robust—more than 75% employ 2FA and hardened passwords, while substantial percentages also employ encryption, biometrics, or cold storage. Additionally, 64% of users indicated a willingness to pay extra fees for more secure protection, highlighting an evident desire for improved protective controls.

By conclusion, although modern cybersecurity in the cryptocurrency platforms would be stopping perceptible breaches at the moment, they are still not seen by a significant proportion of users to be completely up to the job. The conclusions favour the opposite hypothesis that effective, more comprehensive, and elastic security systems have to be there to deal with dynamic digital menaces, and most importantly, with AI and elevated digitalisation-linked threats. There is also a clear suggestion that risk communication and user education need to be enhanced in order to construct more robust trust in the ecosystem.

Even though none of the users have been subjected to a cyber attack and many graded the existing security mechanisms as sufficient, the statistical analysis indicates a considerable gap in perception, particularly a bias towards wanting stronger security systems.

This inconsistency indicates a "preventive awareness" among the user community: they might not have experienced breaches yet, yet numerous expect prospective threats, notably because of AI and digitalisation.

Thus, according to the descriptive analyses, in this research it is concluded that users find present cybersecurity controls on cryptocurrency exchanges and wallets effective hitherto to avoid breaches. But the statistically significant skew in answers, coupled with worry about AI-based threats and cyber vulnerabilities, suggests a robust belief that existing measures might not be adequate in the future.

7.0 RECOMMENDATIONS

- **User Education & Awareness:**

  Crypto platforms should launch targeted campaigns to educate users on cybersecurity risks, phishing, AI threats, and best practices like multi-factor authentication.

- **Stronger Security Frameworks:**

  Integrate AI-driven fraud detection, multi-signature wallets, cold storage, and decentralised exchanges to enhance platform security.

- **Transparent AI Security:**

  Invest in AI-based tools such as biometric and behaviour-based authentication, while ensuring transparency about how these systems function and their limitations.

- **Clear Regulatory Standards:**

India needs defined regulations for crypto cybersecurity, mandating minimum protection standards and supporting ethical AI use while addressing privacy concerns.

- **Cybersecurity Innovation:**

  Adopt blockchain-based ID verification and decentralised authentication. Conduct regular penetration testing to detect and fix vulnerabilities early.

- **Building User Trust:**

  Platforms should perform regular security audits, communicate breaches transparently, and offer premium security services to users willing to pay for enhanced protection.

REFERENCES

- The Economic Times. (2024). Losses from crypto hacks jump to $2.2 billion in 2024, report says.
- CoinLaw. (2023). *Crypto exchange hacks and security statistics*.
- StormWall Network. (n.d.). *Cybersecurity insights and DDoS protection for crypto platforms*.
- Chainalysis Report on Crypto Scams and Hacks (2024)
- CERT-In, CSIRT-Fin, SISA's "Digital Threat Report 2024"
- 2024 Trends: Crypto Adoption and Illicit Exposure by Country- TRM Labs