Indian Journal of Cryptography and Network Security (IJCNS)
ISSN: 2582-9238 (Online), Volume-2 Issue-2, November 2022

The Role of Data Leakage Prevention System in CBDC

Adesh Mukati, Satya Prakash

Abstract*: *A centralized database-based Central Bank Digital Currency (CBDC) system's vulnerability to cyberattacks and data leakage is a major concern. Any data leak can lead to large financial losses, irreversible reputational harm, and a decline in user confidence. To protect user information, the Reserve Bank of India has underlined the significance of a strong Data Leakage Prevention (DLP) system. While current incidents have demonstrated that the measures were insufficient to meet the standards, DLP may not be enough to defend CBDCs on its own. Incorporating Zero-Knowledge Proofs (ZKPs) and differential privacy tools into DLP solutions can improve their robustness and effectiveness. There is no one-size-fits-all solution for preventing data leakage, different solutions may be more effective in different scenarios. It's always a good idea to assess an organization's or system's specific needs and requirements before deciding on the best solution. It is also important to remember that there is no such thing as absolute security, and the possibility of zero-day attacks is always there. It is essential to continuously monitor and enhance security measures to stay ahead of new threats. To preserve their Central Bank Digital Currency systems and data, financial institutions and central banks must continue to be proactive and vigilant.

Keywords*: *CBDC, Data Leakage Prevention System, Differential privacy tools, Zero-Knowledge Proofs (ZKPs).

I. INTRODUCTION

On October 7, 2022, the Reserve Bank of India published a concept note on CBDC (Central Bank Digital Currency) for India. CBDCs are not a novel idea, but it has only been in the last ten years that central banks, governments, and economists have begun to pay serious attention to the concept.[1] Many central banks are exploring the possibility of a digital version of fiat currency. The introduction of CBDCs might reduce the cost of printing, storing, and transferring money. Due to the potential threat posed by the growth of private VCs (virtual currencies), CBDCs are a safe and more reliable kind of digital currency. [2][[3]] The proposed system would use a blockchain-based platform to facilitate secure and efficient transactions, eliminating the need for intermediaries (banks). However, the use of a centralized database in this system is a cause for concern.

Manuscript received on 22 July 2022 | Revised Manuscript received on 05 November 2022 | Manuscript Accepted on 15 November 2022 | Manuscript published on 30 November 2022.
***** Correspondence Author(s)
Adesh Mukati*, Student, Master of Cyber Law and Information Security National Law Institute University, Bhopal (M.P), India. E-mail: adeshmukati.mclis@nliu.ac.in, ORCID ID: https://orcid.org/0000-0001-6449-2508
Dr. Satya Prakash, Assistant Professor, Department of Cyber Law Rajiv Gandhi National Cyber Law Centre National Law Institute University, Bhopal (M.P), India. E-mail: satyaprakash@nliu.ac.in, ORCID ID: https://orcid.org/0009-0007-5866-3607

While all data (transactional and user data) is stored in a single point, centralized databases are susceptible to cyber-attacks and data leakage. This might happen if hackers manage to get past the security safeguards in place and access the database without authorization, potentially resulting in major data loss.[4] For example, in 2018, almost 1.3 million customers of a major Indian bank had their personal information stolen, which was one of the biggest data breaches in the history of the Indian banking industry. However, blockchain systems themselves are not immune to vulnerabilities, and there are potential endpoint vulnerabilities in the Indian CBDC blockchain system that could be exploited by attackers. The security of the entire system might be jeopardized if hackers exploit these vulnerabilities and obtain access to the system, alter transaction data, or steal private keys. There have been several incidents where blockchain-based systems have been hacked and attackers have stolen cryptocurrencies or manipulated transactions. These flaws, which are frequently brought on by endpoint vulnerabilities, let attackers break into the system by taking advantage of weaknesses in individual nodes. One such instance is phishing attacks. Since humans are the weakest link in operational security, individuals or employees of organizations are typically the targets of phishing attacks. This vulnerability causes data leakage, which leads to cyberattacks.[6][7] The Reserve Bank of India (RBI) report's analysis also revealed that the custodian model of token-based wallets may be vulnerable to data loss and leakage. In this model, the TSP (Token Service Provider) is in charge of controlling the wallet's keys on behalf of the user. As a result, the service provider is in charge of keeping user information secure, and the TSP's security protocols' sturdiness determines how secure the tokens are. Although the TSP's reliance on a third party enables recoverability, anonymity may be jeopardized because the service provider will always be aware of the tokens' inflows and outflows from the wallet. Due to the lack of online communication and CBDC's common ledger updates, double spending of tokens is a possibility when using offline functionality. However, this risk can be reduced more effectively through the use of technical solutions and sensible business regulations, such as a monetary cap on offline transactions. The researcher was motivated to conduct this research to identify vulnerabilities in CBDC systems. The aim is to assist policymakers and technology experts in designing more secure and reliable systems that can withstand potential data leakage resulting from various cyber-attacks and ensure the resilience of the CBDC systems.[8]

II. REVIEW OF LITERATURE

• Reserve Bank of India, 'Guidelines on Information Security, Electronic Banking, Technology risk management, and cyber frauds'[9]

The guidelines go over the RBI data protection laws and how businesses must use Data Leakage Prevention (DLP) tools to abide by them. The RBI guidelines require financial institutions to implement appropriate controls to secure confidential data and prevent data breaches. The article emphasizes the significance of implementing DLP solutions that can monitor and manage data transfer as well as prevent data loss through web and email channels.

• Pragya Dhanjika, 'Data Breach in Blockchain Technology'[5]

This research article discusses the potential risks of data breaches in blockchain technology and emphasizes the importance of appropriate security measures and regulations. It also emphasizes the significance of educating users about these risks and implementing best practices for secure data storage and sharing on blockchain networks.

• Sebastian Banescu, Ben Borodach, and Ashley Lannquist, '4 key cybersecurity threats to new central bank digital currencies'[10]

The research article discusses four key threats that central bank digital currencies (CBDCs) may face, including cybersecurity risks, privacy concerns, financial stability concerns, and potential monetary policy consequences. The article urges policymakers to address these issues for CBDCs to be implemented successfully.

• Giulia Fanti and others, 'Missing Key: The challenge of cybersecurity and central bank digital currency'[11]

The report investigates the cybersecurity implications of CBDC issuance, focusing on privacy and financial stability concerns. It lays out regulatory principles for policymakers and emphasizes the importance of collaboration among governments, financial institutions, and technology firms in developing secure CBDCs.

• Peterson K Ozili, 'Central bank digital currency in India: the case for a digital rupee'[12]

This research article investigates India's proposed central bank digital currency, also known as the digital rupee, and assesses the potential benefits and issues that may arise from its implementation. Along with the advantages, this article addresses the security risks that must be evaluated.

III. STATEMENT OF PROBLEM

The Indian CBDC's centralized database, along with the potential endpoint vulnerabilities in the blockchain system, poses a significant risk of data leakage, which is susceptible to data breaches through various cyber-attacks.

IV. HYPOTHESIS

Zero-Knowledge Proofs and differential privacy tools in CBDC effectively prevent data leakage and loss, which ensures robust data security.

V. RESEARCH QUESTIONS

1. Are current DLP systems preventing data leakage and loss in Indian CBDC?
2. Can Zero-Knowledge Proofs and differential privacy tools prevent data leakage risks in centralized blockchain infrastructures?

VI. RESEARCH OBJECTIVES

1. To comprehend the organizations and legislation governing CBDC and data privacy.
2. To analyze the situation of CBDC in India.
3. To determine issues and challenges with a centralized database.
4. To investigate various cyber-attacks on financial institutions and crypto exchanges.
5. To understand the concepts of ZKPs and differential privacy tools.
6. To investigate customers' satisfaction and attitudes toward CBDC.

VII. RESEARCH METHODOLOGY

The research methodology relies on secondary sources to collect data, and the research method employed is exploratory. The researcher aims to determine the effectiveness of ZKPs, differential privacy tools, and DLP in preventing data leakage risks in centralized blockchain infrastructure.

VIII. ROLE OF DATA LEAKAGE PREVENTION SYSTEM

In a CBDC system based on a centralized database, the risk of data loss and cyberattacks is significant.[13] The Reserve Bank of India has emphasized the importance of a strong data leakage prevention system to protect user information from cyber threats and data breaches, as well as the need for organizations to use DLP solutions to comply with these requirements. Before drawing any conclusions, it is critical to assess the effectiveness of current DLP solutions. CBDCs are vulnerable to threats (cyber-attacks, counterfeiting, and fraud) and require a variety of security measures to ensure their integrity and reliability. DLP enforces vulnerability remediation through alerts and protective actions (like encryption to prevent intentional or accidental misuse of sensitive data). DLP software monitors and protects the network, endpoint, and cloud data in motion and at rest.[14]

IX. INCIDENTS OF DATA LEAKAGE, DATA LOSS, AND DATA BREACHES IN THE WORLD OF CRYPTOCURRENCIES

While DLP can help protect CBDCs by reducing the risk of data breaches and unauthorized access to sensitive data, it is not a complete solution. Despite implementing DLP and Security Operations Centre (SOC) measures, cryptocurrency exchanges and financial institutions have experienced security incidents. All the incidents mentioned below have one thing in common, they all involve centralized cryptocurrency exchanges with centralized databases.

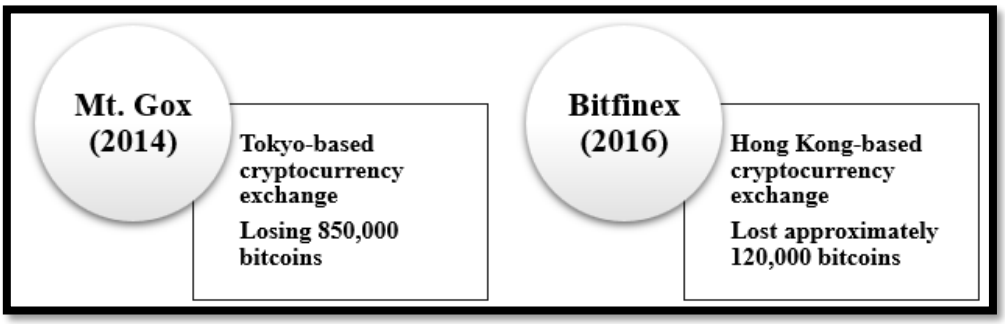

Figure 1 Attack on Cryptocurrency exchanges: (a) Mt. Gox[15] (b) Bitfinex[16]

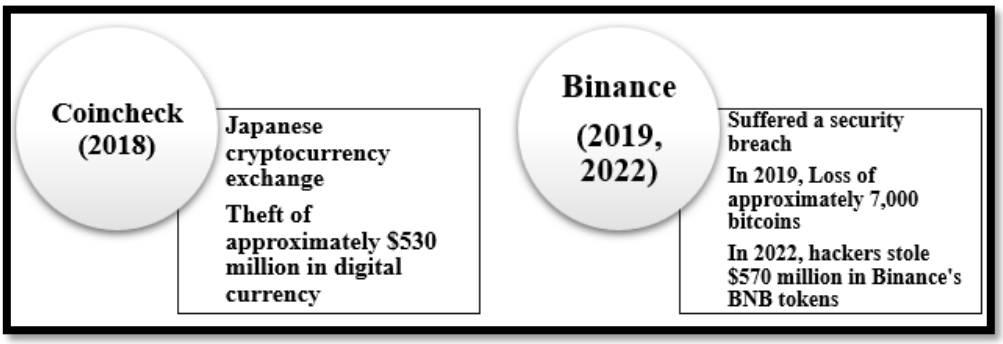

Figure 2 Attack on Cryptocurrency exchanges: (a) Coincheck [17] (b) Binance (2019) [18] (c) Binance (2022) [19]

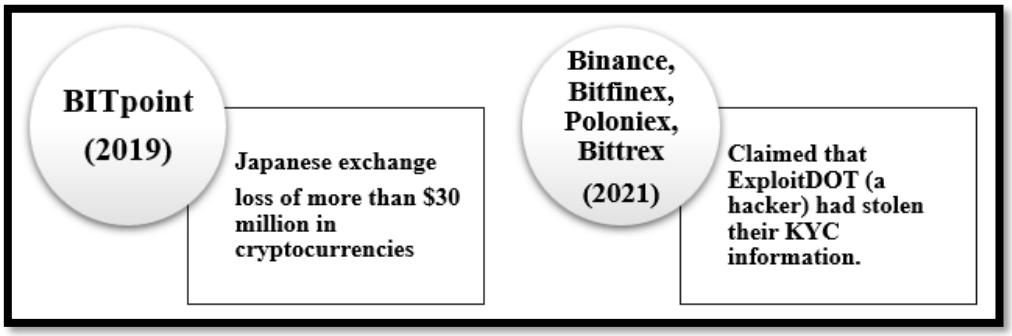

Figure 3 Attack on Cryptocurrency exchanges: (a) BIT point [20] (b) Binance, Bitfinex, Poloniex, and Bittrex [21]

X. VULNERABILITIES OF CENTRALIZED DATABASES

The use of centralized data-sharing systems poses significant risks to security, ethics, and confidentiality. Such architectures create difficulties when attempting to share data between different systems, potentially leading to monopolies. A centralized data system's operation is concentrated in the hands of a single entity, group, or company, making it vulnerable to data leakage and other risks. Furthermore, centralized data systems frequently jeopardize user privacy by sharing user data with third-party entities. Furthermore, centralized data systems are high-value targets for hackers, as they provide them with ample resources to launch attacks while also making them vulnerable to breaches and data theft.

XI. INSIDER THREAT CASE STUDY RELATED TO DIGITAL CURRENCIES

An insider threat is one of the potential data leakage vulnerabilities in CBDC implementation. Insiders in the case of CBDC implementation could be bank employees, contractors, or third-party service providers with access to CBDC data. Insiders may intentionally or unintentionally (in the case of a phishing attack) leak data to unauthorized parties, such as CBDC transaction records, user identification information, or encryption keys. An insider, for example, could steal CBDC encryption keys or copy user identification information and use or sell it to criminals. There have been incidents of insider threats leading to data breaches in the financial sector, including those involving digital currencies.

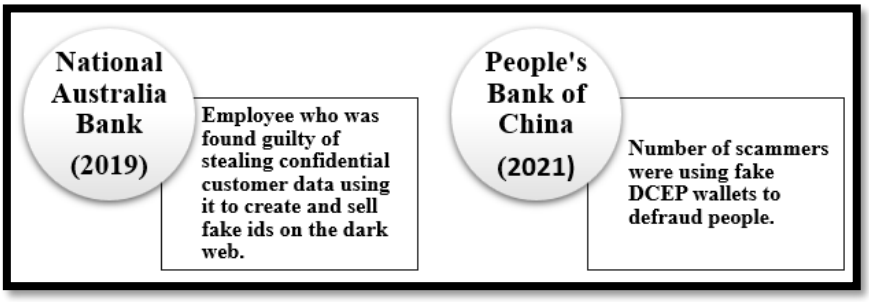

Figure 4 Insider threat case study related to digital currencies: (a) National Australia Bank [22] (b) People's Bank of China[23]

Figure 5 Insider threat case study related to digital currencies: Central Bank of the Bahamas [24]

XII. ZKPS AND DIFFERENTIAL PRIVACY TOOLS

CBDCs are being investigated by central banks all over the world, including the RBI, which has been studying their benefits and drawbacks for some time. The RBI is developing a phased implementation strategy and investigating use cases that will cause minimal disruption, such as the scope of CBDCs, the underlying technology, the validation mechanism, the distribution architecture, and the degree of anonymity. Based on the previous chapter, the researcher concludes that DLP may not be enough to protect CBDCs. Additional security measures must be implemented to protect the system from external attacks and internal fraud.[25]

XIII. EFFECTIVENESS OF ZKPS AND DIFFERENTIAL PRIVACY TOOLS

ZKPs (Authentication Protocol) are cryptographic protocols that allow one party to prove to another that they know a specific piece of information without revealing any additional information beyond what is required. Differential privacy tools, which are a technique for adding noise to data while maintaining privacy and allowing for meaningful analysis, can be used in conjunction with DLP to provide an additional layer of data leakage protection. DLP tools will be used to monitor and control the transfer of sensitive data, while ZKPs will be used to verify the authenticity and integrity of the data being transferred without revealing any more information than is required. This can help prevent data breaches and ensure that only authorized users' access, view, or transmit data. ZKPs could be used in the context of CBDCs to allow users to prove ownership of their CBDC holdings without revealing their actual account balances or transaction histories.

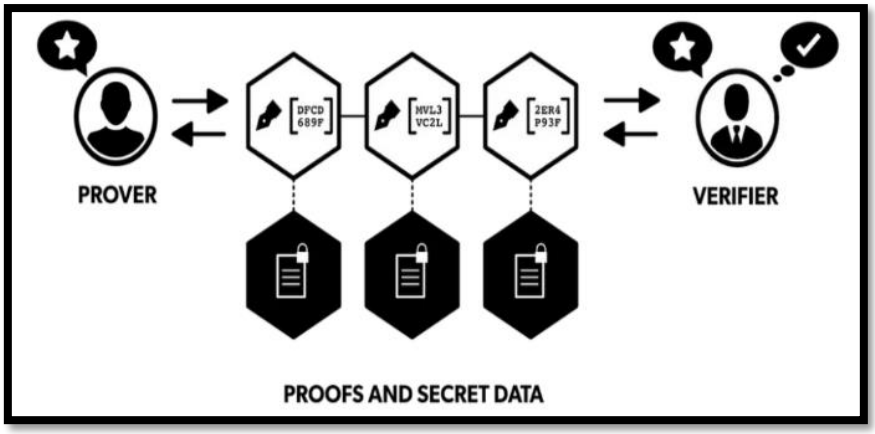

Figure 6 Zero-Knowledge Proof (ZKP) [26]

Differential privacy tools can be combined with DLP tools to improve the privacy of individuals' data. Differential privacy, for example, can be used to add noise to data to protect individuals' identities while still allowing useful insights to be drawn from the data.[27]

A financial institution, for example, may want to protect its customers' personal and financial information while still being able to analyze that data for fraud detection or marketing purposes. The institution can use DLP to implement policies that prevent sensitive information from leaving the network, but it may also be necessary to use Zero-Knowledge Proofs (ZKP) and differential privacy tools to enable secure data analysis without revealing any individual customer information.

By combining these three technologies to limit access to sensitive data, the financial institution can achieve a more comprehensive and secure solution for data protection while still allowing for data analysis, sharing, and preventing unauthorized access and data leakage.

XIV. PREVENTING CENTRALISED BLOCKCHAIN INFRASTRUCTURE

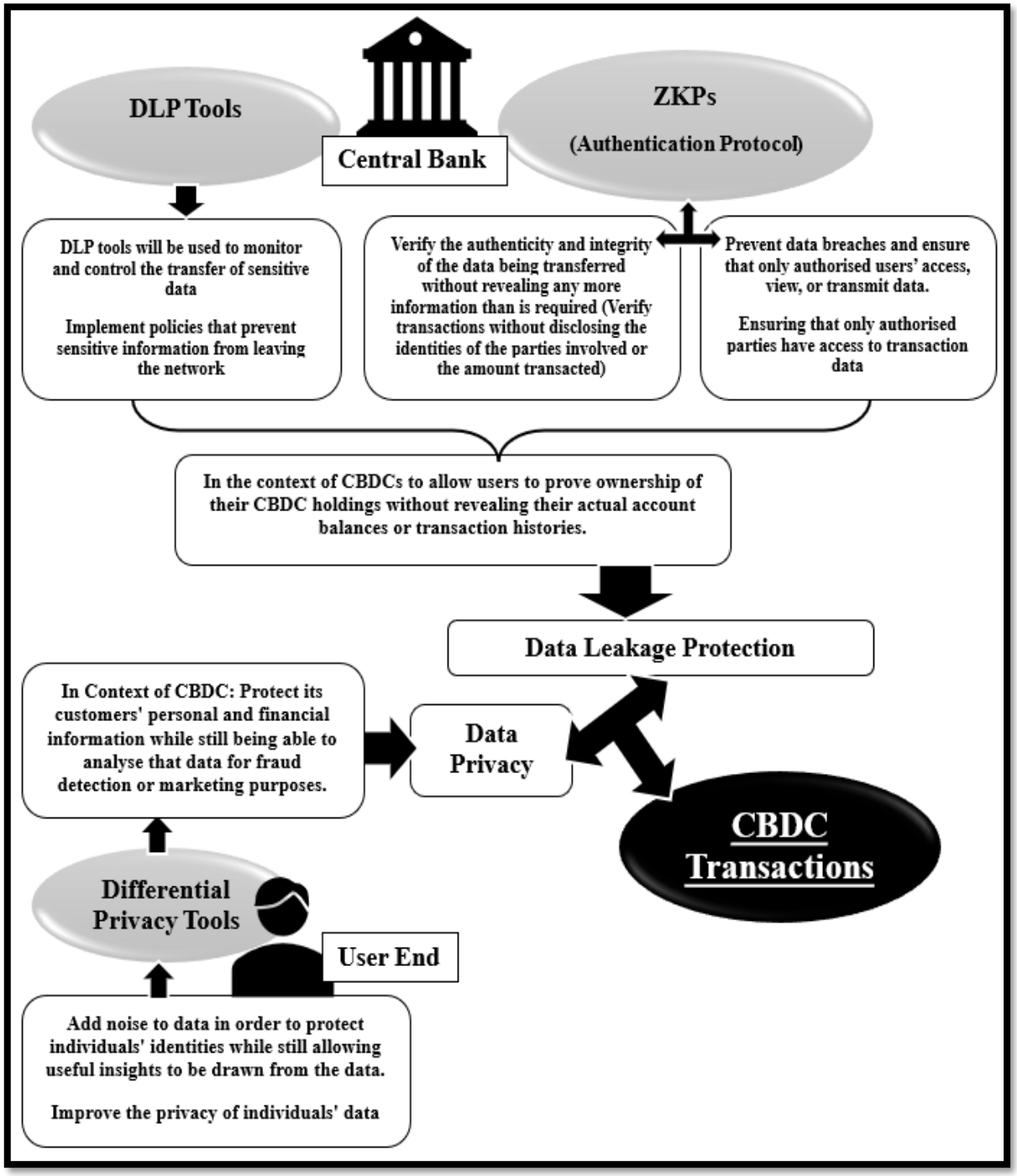

Figure 7 Proposed Model

XV. ADDITIONAL SECURITY MEASURES

Certain measures must also be considered to mitigate the potential risks of data leakage or loss associated with the custody model of token-based wallets and the offline functionality of CBDCs.

1. Token service providers must implement strong security protocols to protect user data and prevent unauthorized access to wallet keys. Two-factor authentication, encryption, and regular security audits are examples of such measures.
2. To ensure user anonymity, token service providers must not collect unnecessary user data and should only access the minimum amount of data necessary to manage wallet keys.
3. Token service providers must update their security protocols regularly to address newly discovered vulnerabilities and stay up to date with the latest security standards.
4. To prevent tokens from being spent twice in offline transactions, appropriate business rules, such as a monetary limit on offline transactions, must be implemented. Furthermore, technical solutions such as time-bound validation of offline transactions are possible.
5. CBDC users must be educated on the potential risks associated with the custody model of token-based wallets and the offline functionality of CBDCs, as well as the steps they can take to mitigate these risks.
6. Token service providers must monitor their systems regularly for potential security breaches and take immediate action to address any vulnerabilities or threats.

XVI. CONCLUSION

After analyzing various incidents, the researcher concluded that DLP is effective but not sufficient to protect CBDC. It should be used in conjunction with additional security measures and best practices to ensure compliance with the RBI guidelines and various regulatory standards, as well as the overall integrity and reliability of the CBDC system. According to the information security principle, complexity is the enemy of security. The solution should be simple to understand but difficult to avoid.

Overall, the security and confidentiality of user data will be critical to the success of the digital rupee (e₹-R) pilot. CBDC implementation poses significant risks, particularly in terms of centralized databases and potential endpoint vulnerabilities that result in data leakage and loss. As a result, the RBI and participating banks must take all necessary precautions to ensure the system's security and protection.

Validity of Hypothesis: The use of ZKPs and differential privacy tools effectively prevents data leakage and loss (even in centralized blockchain infrastructures), ensures robust data security, and protects CBDC users' privacy.

It is also important to remember that there is no such thing as absolute security, and the possibility of zero-day attacks is always there. It is essential to continuously monitor and enhance security measures to stay ahead of new threats.

SUGGESTIONS

1. Conduct regular security audits to identify vulnerabilities and ensure that the CBDC system is secure against potential threats.
2. Educating CBDC users on best practices for data security, such as using strong passwords and avoiding sharing sensitive information.

SCOPE OF FUTURE RESEARCH

The researcher was unable to research the elements listed below due to a lack of resources and time, despite their high research potential. However, the reader is encouraged to do so if they so desire.

1. Examine customer perceptions and satisfaction with CBDC.
2. Investigating the use of decentralized blockchain infrastructure for CBDC.
3. Determine the benefits of artificial intelligence and machine learning in CBDC.

DECLARATION

I, Adesh Mukati, declare that the research paper titled "The Role of Data Leakage Prevention System in CBDC" submitted for publication in the Indian Journal of Cryptography and Network Security (IJCNS) is my original work. I confirm that the research conducted and the writing of the manuscript were carried out by me under the guidance and supervision of Dr. Satya Prakash, who acted as my guide and mentor throughout the research process.

Funding/ Grants/ Financial Support	No, I did not receive.
Conflicts of Interest/ Competing Interests	No conflicts of interest to the best of our knowledge.
Ethical Approval and Consent to Participate	No, the article does not require ethical approval and consent to participate with evidence.
Availability of Data and Material/ Data Access Statement	To successfully carry out the research, the researcher gathered information from secondary sources, including books, law review journals, research papers, journal articles, and newspaper articles. The links to various sources are given in the reference section of this research article.
Authors Contributions	All authors have equal participation in this article.

REFERENCES

1. Sankar T R, 'Central Bank Digital Currency – Is This the Future of Money' (*Reserve Bank of India*, 22 July 2021) <https://www.rbi.org.in/Scripts/BS_SpeechesView.aspx?Id=1111> accessed 24 February 2023.
2. Atlantic Council, 'Central Bank Digital Currency Tracker' (December 2022) <https://www.atlanticcouncil.org/cbdctracker/> accessed 23 February 2023.

3. Rao K S, 'CBDC in India the pros and the cons' *The Hindu businessline* (22 April 2022) <https://www.thehindubusinessline.com/opinion/cbdc-in-india-the-pros-and-the-cons/article65344881.ece> accessed 13 February 2023.
4. Livemint, 'Digital Rupee: Understanding the risks of using digital currency' (13 January 2023) <https://www.livemint.com/money/personal-finance/digital-rupee-understanding-the-risks-of-using-digital-currency-11673593976915.html> accessed 13 February 2023.
5. Dhanjika P, 'Data Breach in Blockchain Technology' (*Amlegals*, 29 December 2021) <https://amlegals.com/data-breach-in-blockchain-technology/#> accessed 12 February 2023.
6. Costa E, 'The Benefits and Vulnerabilities of Blockchain Security' (*CENGN*, 19 October 2021) <https://www.cengn.ca/information-centre/innovation/the-benefits-and-vulnerabilities-of-blockchain-security/> accessed 25 January 2023.
7. Shah M, '5 blockchain security issues and how to prevent them' (*Fast Company*, 16 February 2022) <https://www.fastcompany.com/90722111/5-blockchain-security-issues-and-how-to-prevent-them#:~:text=The%20vulnerability%20of%20blockchain%20endpoints,to%20steal%20the%20user's%20key.> accessed 10 February 2023.
8. Narayan K, 'Digital currency: Cyber security, frauds concerns' *The Indian Express* (9 December 2021) <https://indianexpress.com/article/business/economy/digital-currency-cyber-security-frauds-concerns/> accessed 12 February 2023.
9. Guidelines on Information Security, Electronic Banking, Technology risk management and cyber frauds, 2011, DBS.CO.ITC.BC.No.6/31.02.008/2010-11 30.
10. Banescu S, Borodach B, and Lannquist A, '4 key cybersecurity threats to new central bank digital currencies' (*World Economic Forum*, 20 November 2021) <https://www.weforum.org/agenda/2021/11/4-key-threats-central-bank-digital-currencies/> accessed 20 February 2023.
11. Fanti G and others, 'Missing Key: The challenge of cybersecurity and central bank digital currency' (*Atlantic Council*, 15 June 2022) <https://www.atlanticcouncil.org/in-depth-research-reports/report/missing-key/> accessed 15 February 2023.
12. Ozili P K, 'Central bank digital currency in India: the case for a digital rupee' (*SSRN*, 22 November 2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4238138> accessed 14 February 2023.
13. VarIndia, 'How is CBDC safe from vulnerability and cyber security attacks?' (24 February 2022) <https://varindia.com/news/how-is-cbdc-safe-from-vulnerability-and-cyber-security-attacks-2> accessed 16 March 2023.
14. Cisco, 'What Is Data Loss Prevention (DLP)?' (22 July 2020) <https://www.cisco.com/c/en_in/products/ security/email-security-appliance/data-loss-prevention-dlp.html> accessed 23 February 2023.
15. Mcmillan R, 'The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster' *WIRED* (3 March 2014) <https://www.wired.com/2014/03/bitcoin-exchange/> accessed 11 March 2023.
16. Baldwin C, 'Bitcoin worth $72 million stolen from Bitfinex exchange in Hong Kong' (*Reuters*, 3 August 2016) <https://www.reuters.com/article/us-bitfinex-hacked-hongkong-idUSKCN10E0KP> accessed 11 March 2023.
17. Cheng E, 'Japanese cryptocurrency exchange loses more than $500 million to hackers' *CNBC* (26 January 2018) <https://www.cnbc.com/2018/01/26/japanese-cryptocurrency-exchange-loses-more-than-500-million-to-hackers.html> accessed 11 March 2023.
18. Kharpal A, 'Hackers steal over $40 million worth of bitcoin from one of the world's largest cryptocurrency exchanges' *CNBC* (7 May 2019) <https://www.cnbc.com/2019/05/08/binance-bitcoin-hack-over-40-million-of-cryptocurrency-stolen.html> accessed 11 March 2023.
19. Browne R, '$570 million worth of Binance's BNB token stolen in another major crypto hack' *CNBS* (7 October 2022) <https://www.cnbc.com/2022/10/07/more-than-100-million-worth-of-binances-bnb-token-stolen-in-another-major-crypto-hack.html> accessed 11 March 2023.
20. Zhao W, 'Bitpoint Exchange Hacked for $32 Million in Cryptocurrency' (*CoinDesk*, 12 July 2019) <https://www.coindesk.com/markets/2019/07/12/bitpoint-exchange-hacked-for-32-million-in-cryptocurrency/> accessed 11 March 2023.
21. Raza A, 'The Binance KYC Data Breach: The Hacker Confirms the Attack' *CryptoPotato* (29 March 2021) <https://cryptopotato.com/the-binance-kyc-data-breach-the-hacker-confirms-the-attack/> accessed 11 March 2023.
22. Reuters Staff, 'Australia's NAB says 13,000 customers' personal data breached' (*Reuters*, 26 July 2019) <https://www.reuters.com/article/us-nab-cyber-idUKKCN1UL16P> accessed 13 January 2023.
23. Goh B and Shen S, 'RPT-China's proposed digital currency more about policing than progress' (*Reuters*, 4 November 2019) <https://www.reuters.com/article/china-markets-digital-currency-idUSL3N27H2 AG> accessed 13 March 2023.
24. Soderberg G and others, 'Behind the Scenes of Central Bank Digital Currency: Emerging Trends, Insights, and Policy Lessons' (*IMF eLibrary*, 9 February 2022) <https://www.elibrary.imf.org/view/journals/063/2022 /004/article-A001-en.xml> accessed 13 March 2023. [CrossRef]
25. Alameda T, 'Zero Knowledge Proof: how to maintain privacy in a data-based world' (*BBVA*, 23 June 2020) <https://www.bbva.com/en/zero-knowledge-proof-how-to-maintain-privacy-in-a-data-based-world/> accessed 13 March 2023.
26. Sinha A, 'What are Zero-Knowledge Techniques and Zero-Knowledge Proofs (ZKPs)' (*Medium*, 2 April 2022) <https://medium.com/blockchain-biz/what-are-zero-knowledge-techniques-and-zero-knowledge-proofs-zkps-9e0c236c829e> accessed 16 March 2023.
27. Fathima S, 'Using Differential Privacy to Build Secure Models: Tools, Methods, Best Practices' (*Neptune*, 27 January 2023) <https://neptune.ai/blog/using-differential-privacy-to-build-secure-models-tools-methods-best-practices> accessed 16 March 2023.

AUTHORS PROFILE

Adesh Mukati, Student, Master of Cyber Law and Information Security National Law Institute University, Bhopal Adesh Mukati is a 1st-year student of Master of Cyber Law and Information Security at NLIU, Bhopal, and completed his undergrad in Biochemistry from Govt. Motilal Vigyan Mahavidyalaya, Bhopal. He is a highly motivated individual who is diligently working towards securing a challenging position in a reputable organization. He aims to expand his learning, knowledge, and skills and further develop his professional capabilities. With a strong work ethic and dedication to his career, he is eager to make a valuable contribution to any organization that he joins.
Orcid ID: https://orcid.org/0000-0001-6449-2508

Dr. Satya Prakash, Assistant Professor, Department of Cyber Law Rajiv Gandhi National Cyber Law Centre National Law Institute University, Bhopal Dr. Satya Prakash earned his Ph.D. in Information Technology, Master of Science in Cyber Law and Information Security from IIIT-Allahabad, Prayag Raj, Uttar Pradesh, and LL.B. from the University of Allahabad. Presently, he is working as an Assistant Professor in the Department of Cyber Law, Rajiv Gandhi National Cyber Law Centre, National Law Institute University, Bhopal. He has two and half years of experience in teaching as an Assistant Professor and two years as a Guest Lecturer. He has delivered several lectures on cyber security and the digital forensics domain as a resource person in various workshops nationally and internationally. He is a certified Information Security Management System Auditor/Lead Auditor ISO 27001, A 17226 Certified by IRCA, and Access Data Certified Examiner (ACE). His area of interest includes Information Security, Digital Forensics, Cyber Security, and Cloud Security. Orcid ID: https://orcid.org/0009-0007-5866-3607