Int. j. adv. multidisc. res. stud. 2023; 3(5):798-803

Received: 16-08-2023
Accepted: 26-09-2023

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

An Analytical Study on the Security Features of Digital Payment Systems with Special Reference to Blockchain Technology

[1] Dr. Bhuvana Venkatraman, [2] Harsh Jain

[1] Head & Associate Professor, Department of Commerce Guru Ghasidas VIshwavidyalaya, Bilaspur, Chhattisgarh, India
[2] Research Scholar, Department of Commerce Guru Ghasidas Vishwavidyalaya, Bilaspur, Chhattisgarh, India

Corresponding Author: **Harsh Jain**

Abstract
The internet and technological advancements have revolutionized the financial system. The digital payment system, based on technology, has emerged as a widely popular payment method. The Digital payment system offers users a convenient, fast, secure, and comprehensive payment environment. To use the Digital payment system, the users must take the help of many things, such as a bank account, computer or mobile device, internet, etc. Under the Digital payment system, when any transactions are executed by the users, then the respective transaction has to go through many steps or processes for its successful execution. Since a large section of the present population has become a part of the internet system, huge user data keeps on flowing on the internet. Techniques to protect users' data are developed from time to time, as well as parties known as hackers try to exploit these security techniques by finding loopholes and misusing them. Various methods are used for the authentication of transactions under the Digital payment system, for example, OTP verification, bank authentication, etc. Cryptography and Blockchains are such security technology that is making transactions secure with their different methodologies and working pattern. In this paper, various security features used in Digital payment systems will be explored and security techniques of Blockchain technology will be analyzed analytically. An attempt will also be made in this paper to know the opinion and perceptions of the users about the various security features used under the Digital payment system.

Keywords: Authentication, Blockchain, Cyber-Attacks, Digital Payment System, Security Features, Satisfaction

1. Introduction
The Digital payment system is becoming an integral part of our daily routine. The Indian government has been actively promoting a digital environment through commendable initiatives like the Digital India Mission and the widespread adoption of systems such as e-Rupi and UPI. At present, the Digital payment system has done the work of revolutionizing the finance world. The Digital payment system has worked to promote financial inclusion by providing an accessible, convenient, and easy payment system. However, this transformation is not without its challenges. The surge in digital transactions has attracted cyber threats like cyber-attacks, online frauds, and social engineering, posing considerable risks to the security of the system. Criminals and hackers are making illegal attempts to gather confidential user information through servers and other means for fraudulent activities. To secure online transactions in the Digital payment ecosystem, many security features have been used and updated from time to time. This paper aims to delve into the experiences of users regarding the security features of digital payment systems. By analyzing users' perspectives, it seeks to understand technical issues and opinions related to digital payments comprehensively. Blockchain technology is being employed in numerous sectors, including insurance, real estate, smart contracts, cryptocurrencies, healthcare, and more. This study simultaneously investigates Blockchain technology and Digital payment systems. The research analyzes participants' opinions regarding the use of Blockchain technology with Digital payment systems. Furthermore, it addresses the challenges inherent in each Digital payment system and Blockchain technology, along with their respective features.

2. Review of Literature
(Young Sil Lee *et al*., 2010) [7] In this paper, the authors have presented the model of mobile OTP and QR codes, which can be used in online banking. In the study, the statistics and data of online banking have been described. The modus operandi of OTP and QR code has been explained in detail by the authors. To strengthen the security system of the authentication system, the

authors have proposed their authentication system. In conclusion, the application of their proposed model in the Digital banking system has been explained by the authors, highlighting the security analysis.

(T, 2019) [6] In this paper, the author has described the various dimensions of Digital finance by doing a literary review study about topics like Digital financial inclusion, and fintech, etc., it has been mentioned in the paper that technology-born new tools such as Blockchain, Biometric authentication, Machine learning, Artificial intelligence have changed the financial sector. These technology-driven tools have done the work of bringing many innovative changes. The author has written that different types of Digital finance companies and their products are becoming popular among the people as these products provide simple, easy, convenient, and affordable platforms. The paper describes statistics regarding the growth of fintech market units and fintech products. The conclusion of the paper mentions that the Fintech sector's growth will promote Digital financial inclusion in India with the help of a facilitative and non-discriminatory approach.

(Kaur & Sankhala, 2019) [3] Describing the various prospects and challenges associated with Blockchain technology from the Indian perspective, the authors have said that initiatives are being taken to implement Blockchain technology by many Indian states, citing Andhra Pradesh as an example, it has been told that the possible uses of Blockchain are being explored by Andhra Pradesh for ensuring Digital security and for use in other areas. Regarding Estonia, the authors state that Blockchain is acting as the backbone of Digital e-governance in Estonia. This paper describes the potential utilization of Blockchain in multiple fields/sectors, along with the associated challenges. These challenges encompass aspects like specific vocabulary arrangement specific to this technology, interoperability, data mining costs, scalability, and issues related to protection spillage, all of which are addressed and emphasized within the paper.

(Schuetz & Venkatesh, 2020) [5] In this article, supply chain and financial inclusion have been described the adoption of Blockchain technology in India, it been told in the paper that the main reasons for financial exclusion in India are inappropriate banking products, geographical limitation, financial illiteracy, and high cost, and most of the above problems can be overcome with the help of Blockchain technology. Emphasizing Blockchain technology adoption in India, the authors write that there is a need to take initiatives for the adoption of Blockchain technology in India for financial inclusion. in this paper, a research agenda is developed to link rural Indian supply chains with global supply chains.

(Chahar, Singh, & Hussain, 2023) [1] The authors have studied the components and security features of Digital payment systems and e-commerce in this paper. In the paper, various components of security mechanisms such as confidentiality, integrity, symmetric and asymmetric cryptography, authentication, and access control are described. The authors have proposed to build such a system for micropayments, under which improved security addresses the problems of token payments etc., Authors have proposed a system in which there should be less interaction between the parties so that such a streamlined micropayment system can be generated, in which seller Secure connection can be stabilized between the user and the customer. The authors have also described the protocol for the said system in their article and have broached that the said system will work in four protocol phases and these protocols will include payment token generation, payment token verification, payment phase, and token update and add to Blockchain.

(Chaudhary, Joshi, Bhardwaj, Annu, & Dhiman, 2023) [2] In this paper, the preferences of customers toward Digital payment systems in India have been described. The study describes the various barriers faced by users in the adoption of Digital payment systems such as non-adoption of Digital payments due to lack of new system awareness, fear of financial loss or fraud, etc. In the conclusion of the paper, it has been mentioned that according to various literary analyses, users are giving more preference to card payment under Digital payment. Security seems to be a big point concerning Digital payment to users, as well as infrastructure and slow internet also work to create obstacles in the way of the Digital payment system.

3. Objectives of the Study

1. To overview the various Security features of Digital payment system transactions.
2. To analyze User Experience with different Security Features of the Digital payment system.
3. To Study the awareness and hindrance factors of Blockchain Technology.

4. Research Methodology

This research paper is a Descriptive and Exploratory study, under which the Security features of Digital payment systems and Blockchain technology have been studied. The study utilizes both primary and secondary data collection sources. Primary data was gathered through a circulated Google form, and secondary data was obtained from a variety of sources including online and offline journals, research papers, news websites, government reports, and private publications. Primary data (n=33) has been analyzed with the help of Jamovi & M.S. Excel software.

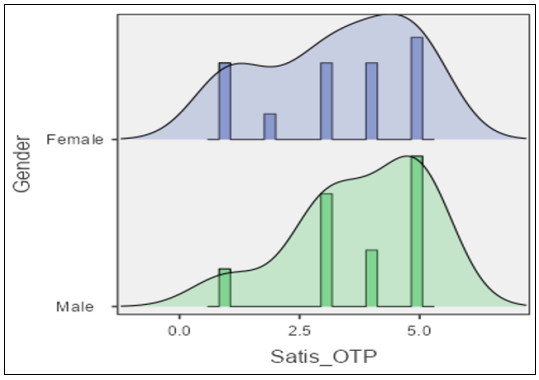
Sample Description: During the study, responses were collected from 33 participants, consisting of 57.6 percent males and 42.4 percent females. The majority of respondents (72.7 percent) fell within the age group of 21-35, while 27.3 percent were below 20 years old. Among the participants, 45.5 percent were doctoral students, 45.5 percent were undergraduates, and 6.1 percent were post-graduates. The student category comprised 81.8 percent of the participants. Additionally, 81.8 percent of the participants reported having a monthly income of less than Rs 20,000.

5. Various Security Features in Digital Payment System

a. **On Device One Time Password:** One Time Password is one of the most prevalent security techniques used within Digital payment systems. Under OTP, a numerical or alphanumerical code is generated for authentication at the time of login session or transactions, which has to be entered by the user in their system, only after that the verification process is completed. Under One Time Password protection technology, a unique passcode is generated for each new transaction or login session. Under the OTP-based authentication process, secret codes are shared between the user's system and the authentication server. OTPs provide stronger security than static passwords, as they

protect users from replay attacks since a unique code is generated each time. OTP generation is done by a special kind of algorithm that uses randomness key generation and a cryptographic hash generator for key generation. The function of a cryptographic hash generator is to derive a value that is difficult to reverse.

To evaluate the satisfaction levels of users of the digital payment system with respect to OTP, data was gathered employing a Likert scale, chosen as the primary method of data collection for this study. Upon analyzing the data using density plots and histograms, a noticeable left-skewed distribution emerged, suggesting a heightened level of satisfaction regarding OTP. Consequently, it can be deduced that both male and female users express higher levels of satisfaction when utilizing OTP as a security measure within the digital payment system.



Source: Authors Computation

Fig 1: Density Plots (Contained within Histograms) Illustrating User Satisfaction Levels with the One-Time Password Security Technique, Segregated by Gender (Male & Female)

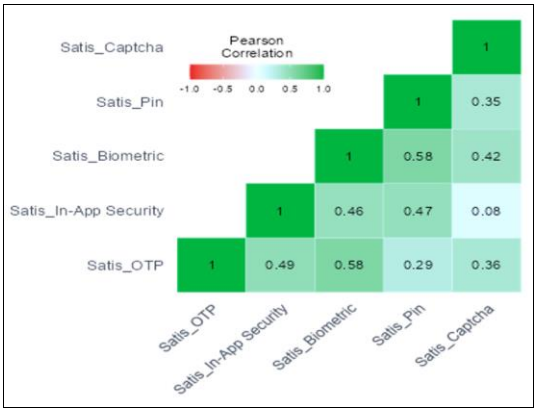
b. In-App Security: In app security features are used by Payment service provider companies within their apps. These features are used to ensure the authenticity and security of Digital transactions and confidential information. For example, Google Pay is using Machine learning systems in its app to protect against fraud and phishing. Payment apps use a variety of mechanisms with these built-in security features, such as the use of biometric authentication to identify users, the use of virtual account numbers to protect the user's card, and the confidentiality of payment information, etc. Payment apps also work to encrypt the data of their app users so that data cannot be breached during payment transit. To reduce the vulnerabilities under these app security features, the work of strong coding is also done by the app's companies so that a clear clearing mechanism can be created. Multi-level authentication is also used for security during the use of payment gateway under these app security features. Upon analyzing the primary data collected during the study, it was discovered that approximately 33 percent of users encounter technical difficulties specifically related to the in-app security features while utilizing Digital payments. This percentage is higher compared to the other security aspects of our study.

c. Device-based Biometric Authentication: Under Device based biometric authentication, human biological features such as iris scan, fingerprint scanning, and facial recognition are used for verification. Features such as scanning mechanisms and sensors are used in devices for biometric authentication. Due to the use of biological identity, this security technology provides more security to the users as compared to PIN. During Digital payment, the user's data pre-stored in mobile or other gadget is matched through biometric verification, the transaction becomes successful in the direction of a successful match.

d. PIN (Personal Identification Number): Personal Identification Number or PIN refers to such a security technique, under which verification is done with the help of numeric or alphanumeric codes for authentication. The PIN is a widely used security technology tool. PIN is being used by almost all payment and fintech companies in some form or the other. At present, both PIN and OTP are being used to provide more security to the users under the two-factor authentication system in use. Sometimes, PINs become vulnerable to misuse due to their static nature. Currently, a tokenization system is being employed to enhance security alongside PINs. In this system, transactions are completed using a token instead of entering a PIN.

e. Robot Verification: Robot Verification or CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Human Apart) is used under Digital Payment System to check and verify whether the execution of transactions is done by humans or not. These security features are used to protect transactions from unauthorized access and automated attacks. Under robot verification or captcha verification, texts, images, etc. are tested for verification, sometimes testing is also done through arithmetic questions in this process. Presently captcha verification system is being used in most of the payment gateways**.**

Correlation Heatmap Showing Level of Correlation among Security Features in Digital Payment system



Source: Authors Computation

Fig 2: The correlation heatmap illustrates the relationships and correlations among various security features in terms of user satisfaction

By Analyzing the data obtained in the study regarding the security features of the Digital payment system, it depicts that all these features are positively correlated with each other. The high degree of correlation is not visible between the security features, Data indicates a low to moderate level of correlation. Therefore, it can be inferred that the satisfaction levels of Digital payment system users are affected by various security features, and these security

features are positively (low to moderate level) correlated with each other.

6. Hypothesis Testing

H_0: There is not any significant difference between the Satisfaction level of Males and Female regarding various security features of Digital payment system.

H_1: There is a significant difference between the Satisfaction level of Males and Female regarding various security features of Digital payment system.

Table 1: Tests of Normality

		statistic	p
Satisfaction level OTP	Shapiro-Wilk	0.903	0.006
Satisfaction level In-App Security	Shapiro-Wilk	0.890	0.003
Satisfaction level Biometric	Shapiro-Wilk	0.887	0.002
Satisfaction level Pin	Shapiro-Wilk	0.857	< .001
Satisfaction level Robot Verification	Shapiro-Wilk	0.946	0.099

Source: Authors Computation

Test of Normality depicts that data is normally distributed because the value of Shapiro Wilk is >0.07

To assess the disparity in satisfaction levels between males and females, it is essential to conduct an independent sample T-Test

Table 2: Independent Samples T-Test

		Statistic	df	p
Satisfaction level OTP	Student's t	-1.0112	31.0	0.320
Satisfaction level In-App Security	Student's t	0.3104	31.0	0.758
Satisfaction level Biometric	Student's t	-0.4185	31.0	0.678
Satisfaction level Pin	Student's t	0.0653	31.0	0.948
Satisfaction level Robot Verification	Student's t	-0.5329	31.0	0.598

Source: Authors Computation

Interpretation

An independent-samples t-test was performed to assess the satisfaction level of security features such as OTP, In-App Security, Biometrics, PIN, and Robot Verification among males and females. The t-test results indicated that for all security features, the p-value exceeded 0.05, leading us to accept the null hypothesis.

Based on this hypothesis, it can be inferred that there is no significant difference in the satisfaction levels between males and females regarding the various security features of the Digital payment system.

7. Blockchain and Digital Payment System

Blockchain technology is widely utilized for diverse purposes, such as facilitating smart contracts, enabling cryptocurrency operations, and enhancing supply chain management. Within the realm of the Digital payment system, Blockchain offers the potential to establish a transparent, highly secure, cryptographically robust, and decentralized payment system. The distinctive characteristics of Blockchain, including its peer-to-peer network-based structure, decentralized nature, and employment of cryptographic security techniques, distinguish it from traditional payment systems. As a contemporary technology, Blockchain continues to be explored for novel applications across various fields. In the study, participants were surveyed using a Likert Scale to assess their awareness of Blockchain technology's implementation in different domains. Based on the analysis of these responses, the following conclusions were derived and are presented in the Table 3 for further elucidation.

After analysing the Table 3 responses, the following conclusions are obtained, which are explained with the help of the Table 4.

Table 3: Users awareness level regarding Use of Blockchain Technology in various sectors

	Gender	Finance	Account	Cloud Computing	Healthcare	Insurance	Real Estate	Crowdfunding
Mean	Female	3.00	3.21	2.86	2.86	2.64	2.79	2.50
	Male	3.58	3.58	3.53	3.21	3.42	3.42	3.37

Source: Authors Computation

Table 4: Interpretation of Awareness Level (males and females)

	Finance	Account	Cloud Computing	Healthcare	Insurance	Real Estate	Crowdfunding
Male	N.A.	N.A.-H.A.	L.A.-N.A.	L.A.-N.A.	L.A.-N.A.	L.A.-N.A.	L.A.-N.A.
Female	N.A. -H.A.	N.A.-H.A.	N.A.-H.A.	N.A.-H.A.	N.A.-H.A.	N.A.-H.A.	N.A.-H.A.
Legends:	N.A. = Neutral Awareness L.A.= Low Awareness H.A.= High Awareness						

Cryptocurrency, a form of digital currency built on Blockchain technology, operates within a decentralized system where transactions are recorded in the form of blocks. Authentication of cryptocurrency transactions occurs through peer-to-peer networks. Being decentralized, cryptocurrencies are not subject to governmental control, and they lack underlying assets. The unregulated nature and absence of underlying asset banking contribute to significant price volatility and hype surrounding cryptocurrencies.

The participants were queried to identify the obstacles associated with the utilization of cryptocurrencies. Analysis of the participants' responses revealed that the majority expressed neutral opinions. It appears that the participants held neutral views on various factors on the use of cryptocurrencies.

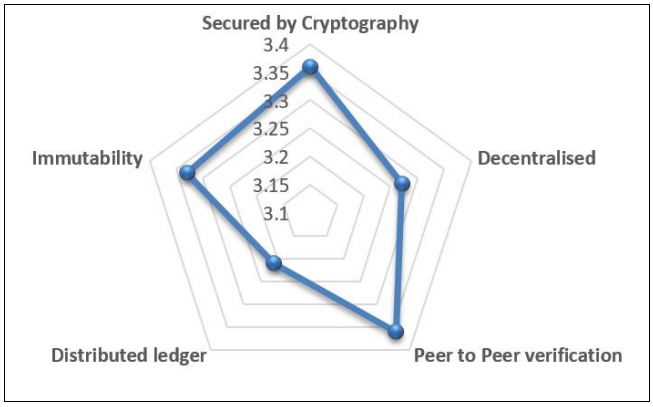
Table 5: User assessments regarding impediments associated with the utilization of blockchain-based cryptocurrencies

	Price Volatility	Not Regulated	Tracking	Decentralization	Misuse	No Reversal	Legal Protection
Mean	3.26	3.06	3.34	3.34	3.16	3.16	3.35
Standard deviation	1.12	1.12	1.12	1.12	0.987	1.11	1.20

Source: Authors Computation

From the analysis of the above table, it is known that most of the participants are neutral regarding the said hindrance factors.

To evaluate the potential of Blockchain technology as a superior payment system within the Digital payment system, we inquired with the participants regarding the specific security features of Blockchain that they believe could contribute to its establishment. We gauged participants' opinions using a Likert scale. The resulting conclusion and its corresponding explanation are as follows:



Source: Authors Computation

Fig 3: A radar graph illustrates the impact of diverse attributes of Blockchain technology, as perceived by respondents, on fortifying Blockchain as a more resilient verification and authentication technique within the Digital payment system in the future

From the analyses of the said radar graph, it is observed that users have responded in neutral to high-impact level areas, from the analysis of these areas, it can be understood that according to user's peer-to-peer verification, cryptographic security, and immutability features of Blockchain are impactful towards establishing a better Digital payment system in the future.

8. Findings & Conclusion

Findings

- Out of 33 respondents in the study, 32 respondents reported that they are users of Digital payment systems.
- 7 out of 33 respondents of the study told that the main reasons behind not using the Digital payment system are technical problems during Digital payment, the availability of cash as a better payment system, and their work can also be done without Digital payment.
- 42.4 percent of respondents of the study do 5-20 Digital payment transactions in a month, 21.2 percent do 20-35 Digital payment transactions, 15.2 percent do 35-50 Digital payment transactions and 15.2 percent do more than 50 Digital payment transactions in a month.
- Data Reveals that under the Digital payment system, the Unified Payment Interface is used by a maximum of 97 percent of the users for Digital payment.
- Regarding the security features under the Digital payment system, 45.5 percent of the participants consider PIN as a convenient and comfortable feature. The same 21.2 percent consider in-app security, 15.2 percent device-based biometric authentication, and 15.2 percent on-device OTP as convenient and comfortable security features.
- Based on the data provided by the respondents, it is evident that 33.3 percent of the respondents encounter technical difficulties with in-app security features, while another 33.3 percent face issues during robot verification or captcha verification. Additionally, 21.2 percent of the participants experience technical challenges during OTP verification.
- Server issues, poor connectivity, time-outs, and unnecessary pop-ups are some of the main problems faced by the respondents during Digital payment system transactions.
- 54.5 percent of respondents are satisfied with the current security techniques used under the Digital payment system, while 42.5 percent of participants have no clear opinion (neutral) in this regard. The remaining 3 percent are not satisfied with the current security techniques used under the Digital payment system.
- Among the respondents, 72.8 percent agree to strongly agree that the incorporation of blockchain technology will enhance the effectiveness of Digital payment system, whereas 24.2 percent of participant expressed no definitive opinion on this, the remaining 3 percent of participant strongly disagree with this notion.

Conclusion

The Digital payment system is a rapidly expanding ecosystem, but users currently encounter technical difficulties with multiple security features that necessitate resolution by payment system companies and banks. Poor internet connectivity and a lack of proper knowledge of Digital payments in the country are challenges in the development of a Digital payment system. For this, there is a need to develop infrastructure. Blockchain technology is being used in various fields, there is a need for research and testing for the use of Blockchain technology with Digital payments. The specific security features of Blockchain technology can contribute to the development of Digital payment systems. It is expected that in the future, both the Digital payment system and the Blockchain system will work synergistically implementing necessary technical advancements to address present and future challenges in these systems.

Furthermore, fostering digital literacy and awareness campaigns can play a pivotal role in addressing the knowledge gap and ensuring a smoother transition to digital payment methods. Collaborations and partnerships between industry stakeholders and government bodies are essential to address infrastructural gaps and ensure a robust digital payment ecosystem. Rigorous testing and analysis of the integration of Blockchain technology with digital payments will be crucial in unlocking its full potential and ensuring seamless and secure transactions. Moreover, ongoing research and development efforts should focus on enhancing the scalability, efficiency, and security of both digital payment systems and Blockchain technology to keep up with evolving cyber threats and user demands

9. Limitation and Future Research Scope

- The number of sample sizes in this study is 33, and the conclusions may be affected if analysis is done on more samples.
- Within the purview of this study, a meticulous analysis has been undertaken concerning specific security features affiliated with Digital payment systems. It is essential to underscore that the study may benefit from

an exploration of supplementary security features for potential inclusion.

- A significant portion of the study's participants represents the student community. It is imperative to acknowledge that the conclusions drawn from this study may be influenced by this demographic bias. To enhance the robustness and generalizability of the findings, future research endeavors should strive to diversify the participant pool by incorporating data from other relevant communities.

10. References

1. Chahar NK, Singh KP, Hussain M. Simplified Micropayment Mechanism to Eliminate the Risk of Double Payment in E-Commerce. International Conference on Advances in Intelligent Computing and Applications (AICAPS), 2023. Doi: 10.1109/AICAPS57044.2023.10074490
2. Chaudhary DG, Joshi S, Bhardwaj V, Annu, Dhiman A. An investigation of the customer preferences towards Digital payments in india. International Research Journal of Modernization in Engineering Technology and Science, 2023, 3543-3551.
3. Kaur A, Sankhala VS. Blockchain Technology in India-Prospects and Challenges. IOSR Journal of Economics and Finance (IOSR-JEF), 2019, 28-40.
4. Prawira KT, Makmur A, Santoso H. Enterprise Architecture for Payment System Industry in Industrial Era 4.0. Sinkron: Jurnal dan Penelitian Teknik Informatika, 2023, 517-525.
5. Schuetz S, Venkatesh V. Blockchain, adoption, and financial inclusion in India: Research opportunities. International Journal of Information Management. 2020; 52:p101936. Doi: https://doi.org/10.1016/j.ijinfomgt.2019.04.009
6. TR. Digital Financial Inclusion: A Payoff of Financial Technology and Digital Finance Uprising in India. International Journal of Scientific & Technology Research, 2019, 3434-3438.
7. Young Sil Lee, Nack Hyun Kim, Hyotaek Lim, HeungKuk Jo, Hoon Jae Lee. Online banking authentication system using mobile-OTP with QR-code. 5th International Conference on Computer Sciences and Convergence Information Technology, 2010, 644-648. Doi: https://doi.org/10.1109/ICCIT.2010.5711134
8. The jamovi project. *jamovi.* (Version 2.3) [Computer Software], 2022. Retrieved from: https://www.jamovi.org.