Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 6, pp. 2539–2549
DOI : 10.47974/JDMSC-2338

Study on encryption techniques for secured online payment system

Saurav Kumar [‡]
Gagan Deep Chadha [@]
Faculty of Business Management
Sarala Birla University
Ranchi 835103
Jharkhand
India

Aditya Vikram Agarwal [†]
Orbit Systems Inc
Columbus 43235
Ohio OH
United States

Rajat Goel [§]
Department of Computer Science and Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Naresh Kedia *
Department of Business Administration
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Abstract

In the digital era, securing payment methods is crucial for protecting financial transactions within India's financial sector. Encryption plays a vital role by converting

[‡] *E-mail:* sauravsingh0028@gmail.com
[@] *E-mail:* gagan.d.chadha@gmail.com
[†] *E-mail:* adityavagarwal.research@gmail.com
[§] *E-mail:* rajat.goel@jaipur.manipal.edu
* *E-mail:* naresh.kedia@jaipur.manipal.edu (Corresponding Author)

© Taru Publications

sensitive data into secure codes, making it inaccessible to unauthorized parties. This, combined with authentication measures like two-factor authentication (2FA) and biometric verification, ensures that only authorized individuals can initiate transactions. Additionally, advanced fraud detection systems monitor suspicious activities, enhancing security. As India's digital economy grows, particularly in mobile payments and online banking, robust encryption standards are essential for maintaining trust and safeguarding the payment system's integrity. Together, these components maintain consumer trust and protect the integrity of India's banking system in the digital age.In this study a sample of 267 is collected from banking sector employees. The factors that identify essential elements of secured payment system are Encryption, Authentication, Integrity, and Fraud Detection and Prevention.

Subject Classification: *Primary 68R01, Secondary 97N70.*

Keywords: *Secured payment methods, Encryption, Authentication, Fraud detection, Financial transactions, Digital economy, Mobile payments.*

Introduction

When it comes to e-commerce and mobile payments in particular, a secure payment system is essential to preserving customer confidence. Encryption methods that are strong and protect sensitive financial data during transactions are one of the key components of these kinds of systems. In order to safeguard user data from potential cyber threats, paper [7] claim that the fast evolution of mobile payment platforms in India has made the adoption of sophisticated encryption techniques necessary. Data is rendered unreadable via encryption, which acts as a vital defense mechanism to keep information unreadable even in the event that it is intercepted. Encryption technologies like Transport Layer Security (TLS) and Secure Sockets Layer (SSL) are essential for preserving Ensuring the privacy and accuracy of data during transmission. Which improves the overall security of the payment platform?

User authentication plays an important function in a secured payment system in addition to encryption. Multi-factor authentication, or MFA, is important for forecasting whether or not an Indian will use mobile banking services [8]. A blend of the user's expertise and understanding. (such as a password), their possessions (such a mobile), and their knowledge (biometric verification) are usually used in multi-factor authentication (MFA). It is improbable that unauthorized access to the payment system will occur even in the event that one component of the security system is hacked thanks to the layered approach. Verified users can only access critical information in a secure environment that is created by encryption

and authentication systems working together. Because encryption and authentication work together to enhance security, mobile banking platforms' security frameworks are strengthened, which promotes user adoption by giving users confidence that their data is protected [9].

Integration of encrypted secure payment methods is critical to maintaining the integrity of the e-commerce ecosystem. The growing popularity of e-commerce has brought attention to the necessity of safe electronic payment methods that can reduce the dangers involved in conducting business online, as noted in paper [2]. To avoid unwanted access and data breaches, encryption technologies are essential in assuring the safe transmission of payment information between the merchant and the customer. Furthermore, by preventing both the buyer and the seller from disputing the transaction's legitimacy, encryption aids in the maintenance of non-repudiation of transactions. Because e-commerce eliminates the need for in-person interaction and thus lowers the danger of fraud, this feature is very crucial. A secure and reliable payment procedure is a must for the continued expansion of online marketplaces, and e-commerce platforms can provide it by utilizing robust encryption techniques.

Literature Review

In India, consumers' intentions to accept "mobile payment systems" are heavily impacted by their perceptions of "security," claim in [4]. In this situation, "encryption" offers a vital degree of security by making sure that transaction data is difficult for unauthorized parties to read or decode. By transforming information into a coded format, "encryption" contributes to the preservation of the integrity and privacy of financial transactions, which in turn builds customer confidence in "mobile payment platforms." They highlighted the critical role that "encryption" plays in propelling the adoption of digital payment systems in the Indian market, where security concerns are important. One essential instrument for maintaining the integrity and secrecy of financial data is encryption. Paper [3] talk about how consumer happiness is affected by the quality of internet banking services, they emphasize that transaction security is a crucial part of that quality. In order to keep sensitive data safe from online attacks, like account details and personal identification numbers (PINs), encryption is essential. Encryption secures individual transactions in the context of online banking while also maintaining public confidence in the financial institution. Banks may minimize the risk of fraud and data breaches by

encrypting data at every stage, including when it's being kept on computers and transmitted across networks.

A "secured payment system" must also seamlessly integrate "encryption protocols" with user-friendly interfaces to improve overall security without sacrificing user experience. Singh and Srivastava [8] investigate the perceptions of current Indian online banking clients on the use of "mobile banking," indicating that "encryption" plays a significant role in their decision to utilize these services. They emphasize how "encryption" shields private financial information from prying eyes and gives consumers peace of mind about the security of their transactions. Financial institutions can provide a safer environment for transactions by implementing strong "encryption protocols," which therefore raises the possibility that users will embrace "mobile banking." The smooth incorporation of "encryption" into the payment system guarantees that users receive improved security features without needless complication, which enhances user happiness in general.

The significance of "encryption" increases when considering "mobile banking adoption," especially when considering younger users in developing nations like India. Encryption is a vital component that makes mobile banking safe [6]. It is observed that younger consumers—who are more technologically literate and drawn to digital solutions—place a high value on the "security" characteristics that "encryption" technologies offer. Assuming that their financial information is secured and shielded from unwanted access increases the likelihood that these customers will use "mobile banking" services. The authors contend that the significance of "encryption" will only grow as "mobile banking" develops, making it a vital component of safe financial transactions. Financial organizations and banks can safeguard their clients and encourage wider use of "mobile banking" services by prioritizing "encryption" in security protocols.

Paper [10] asserts that the demonetization phase in India greatly spurred. The evolution of digital payment systems, highlighting the necessity of strong security measures to safeguard private financial information. A secure payment system must have "authentication," "confidentiality," "integrity," and "non-repudiation." These elements guarantee that data stays private and unmodified during transmission, that parties cannot dispute their involvement in a transaction, and that only authorized personnel can access the payment system. It highlights the value of multi-factor authentication, which uses three factors to confirm identity: the user's knowledge (password), possessions (such as a Smartphone), and identity (such as a fingerprint). Moreover, encryption is

essential for preserving the integrity and secrecy of the data that is transferred via these systems. Encryption guarantees that even if data is intercepted, Intercepted, it remains unavailable to unauthorized users, it is converted into an encoded format that can only be deciphered using a specific decryption key.

Encryption is essential for safeguarding sensitive data. involved in transactions, especially in the financial sector. In paper [1], the banking industry has seen a notable increase in sales as a result of the growth of e-payments and online shopping. This development has been advantageous, but it has also raised the possibility of problems related to cyber threats. Establishing a safe environment for digital transactions requires the use of sophisticated encryption protocols like "Transport Layer Security (TLS)" and "Secure Sockets Layer (SSL)." By creating an encrypted connection between the user's browser and the bank's server, these protocols guarantee the security and privacy of any data exchanged between the two. Additionally, they made the point that while encryption guards against external dangers, it also contributes to the development of consumer trust, as people are more willing to transact online when they feel secure in the knowledge that their financial and personal data is protected. As a result, in the digital era, encryption plays an important role in banking and is not only technically necessary but also strategically imperative for promoting growth and preserving client loyalty.

"Perceived security," or the users' faith in the system's ability to shield their private data from intrusions or breaches, is one of the fundamental components. Users' propensity to stick with digital payment methods like M-wallets is significantly influenced by their level of confidence. Paper [5] stress that the sense of security is even more crucial in developing nations where technology literacy and trust in digital systems may still be emerging. To safeguard data during transmission and storage, a secured payment system needs to have cutting-edge security features like encryption. By transforming data is transformed into an encoded format that only authorized individuals can decrypt. Encryption serves as a protective barrier that keeps unwanted access from happening. This aspect of encryption helps to maintain the use of digital payment systems by fostering user trust and protecting the transaction. Additionally, multifactor authentication which demands users to prove their identity through several channels—is frequently integrated into secure payment systems, further boosting security and user confidence.

Objective

To identify "Essential Elements of Secured Payment System in financial industry"

Study's Methodology

The study includes respondents selected from employees in the banking sector. Random sampling method was used to collect data and examined by "Explanatory Factor Analysis" for results.

Findings of the Study

The table below presents the demographic details of the participants. It indicates that 52.43% are male, while 47.57% are female. Regarding the respondents' age, 37.08% fall within the 35 to 40-year range, 26.59% are between 40 and 45 years, and 36.33% are above 50 years. In terms of the banking sector distribution, 31.09% belong to private banks, 37.83% to public banks, and 31.08% to regional rural banks. Details of the respondent are listed in Table 1. Along with that table 2 provide the value of KMO and Bartlett's Test**.**

Details of Respondent

Table 1

"Factor Analysis"

Variable	Participants	% age
Gender of Participants		
Male	140	52.43%
Female	127	47.57%
Total	**267**	**100**
Age in years		
35 to 40	99	37.08%
40 to 45	71	26.59%
Above 50	97	36.33%
Total	**267**	**100**
Banking sector		
Private banks	83	31.09%
Public banks	101	37.83%
Regional Rural banks	83	31.08%
Total	**267**	**100**

"KMO and Bartlett's Test"

Table 2

"KMO and Bartlett's Test", value of KMO is .779

"Kaiser-Meyer-Olkin Measure of Sampling Adequacy"		.779
"Bartlett's Test of Sphericity"	"Approx. Chi-Square"	4570.627
	Df	91
	Significance	.000

"Total Variance Explained"

Table 3

Result Analysis

"Component"	"Initial Eigenvalues"			"Rotation Sums of Squared Loadings"		
	"Total"	"% Of Variance"	"Cumulative %"	"Total"	"% Of Variance"	"Cumulative %"
1	6.294	44.956	44.956	3.749	26.78	26.78
2	2.526	18.042	62.998	3.688	26.343	53.123
3	2.002	14.298	77.296	2.529	18.065	71.188
4	1.419	10.139	87.434	2.274	16.246	87.434
5	0.46	3.283	90.718			
6	0.416	2.973	93.691			
7	0.243	1.735	95.426			
8	0.179	1.281	96.707			
9	0.155	1.105	97.813			
10	0.122	0.872	98.685			
11	0.065	0.467	99.152			
12	0.055	0.391	99.543			
13	0.041	0.293	99.836			
14	0.023	0.164	100			

The result is shown in Table 3 and 4. All four factors contribute to explaining a total variance of 87.434%. The variance explained by Encryption is 26.780%, Authentication accounts for 26.343%, Integrity contributes 18.065%, and Fraud Detection and Prevention explains 16.246%.

Table 4

Scree Plot - "Rotated Component Matrix"

S. No.	Statements	Factor Loading	Factor Reliability
	Encryption		0.958
1	Ensures that sensitive datais securely transmitted between parties	0.954	
2	Prevents unauthorized access and ensures confidentiality	0.89	
3	Includes symmetric encryption and asymmetric encryption	0.884	
4	Encryption is crucial for protecting data at rest and in transit	0.874	
	Authentication		0.968
1	Authentication mechanisms verify the identity of the users involved in a transaction	0.958	
2	Include passwords, biometric verification two-factor authentication and multi-factor authentication	0.926	
3	Utilization of digital certificates issued by reputable certification authorities.	0.91	
4	Verify the identities of the parties participating in the transaction.	0.905	
	Integrity		0.883
1	Mechanisms such as hashingensure that the data has not been altered during transmission	0.905	
2	Guarantees that the information received is exactly what was sent	0.847	
3	Digital signatures provide proof of origin and integrity of the transaction data	0.826	
	Fraud Detection and Prevention		0.832
1	Real-time transaction monitoring helps detect and prevent fraudulent activities.	0.927	

Contd...

2	Using AI and machine learning to analyze transaction data for potential fraud	0.925	
3	Advanced fraud detection systems monitor suspicious activities, enhancing security	0.638	

Factors and the corresponding variables

Encryption is the initial factor of the study, it includes variables like Ensures that sensitive data is securely transmitted between parties, prevents unauthorized access and ensures confidentiality, includes symmetric encryption and asymmetric encryption, and Encryption is crucial for protecting data at rest and in transit. Second factor is Authentication, the variables it includes are Authentication mechanisms verify the identity of the users involved in a transaction, include passwords, biometric verification two-factor authentication and multi-factor authentication Utilizing digital certificates issued by trusted certification authorities to verify the identities of the parties involved in the transaction. Third factor is Integrity, its variables are Mechanisms such as hashing ensure that the data has not been altered during transmission, guarantees that the information received is exactly what was sent, and Digital signatures provide proof of origin and integrity of the transaction data. Last and fourth factor is Fraud Detection and Prevention, variables under this factor are Systems monitor transactions in real-time helps in detecting and preventing fraudulent transactions, Using AI and machine learning to analyze transaction data for potential fraud, and Advanced fraud detection systems monitor suspicious activities, enhancing security.

"Reliability Statistics"

Table 5

"Cronbach's Alpha"	"Number of Items"
.897	14

Table 5 shows the total reliability of 14 items that include variables for essential Elements of Secured Payment System in Banking is 0.897.

Conclusion

In conclusion, the provision of a secure payment mechanism is a vital requirement for preserving clients' trust and confidence in the digital

banking ecosystem. Protecting sensitive financial data against cyber threats and unauthorized access has become more important than ever in today's connected world where online transactions are the standard. In this sense, encryption is crucial because it forms the basis of digital payment systems' security. Encryption ensures that only authorized parties can access and understand data by converting it into an unreadable format. unreadable format. This conversion successfully stops fraud, data leaks, and other nefarious acts that can jeopardize the accuracy of financial transactions. Symmetric and asymmetric encryptions are two types of encryption that are intended to offer strong defense against online fraud. Symmetric encryption is effective for handling massive amounts of data since it employs the same key for both encryption and decryption. By guaranteeing that only the intended receiver can decrypt the message, asymmetric encryption, on the other side, uses a pair of keys—public and private—to provide an additional degree of protection. Sensitive financial information is kept private and secure since it is very difficult for unauthorized parties to compromise systems due to the intricacy of these encryption techniques. One cannot emphasize how crucial encryption is to preserving the security and integrity of payment systems as digital transactions continue to grow in number. Cybercriminals are growing more skilled in their techniques, and cyber risks are always changing. It is therefore crucial that banks and other financial organizations constantly modify and improve their encryption policies. It takes constant investment in cutting-edge encryption technologies and a proactive approach to security to stay ahead of new threats. Through this approach, financial institutions can guarantee a dependable and secure banking encounter for every customer, thereby strengthening their faith in the digital financial landscape. The factors that identify essential elements of secured payment system are Encryption, Authentication, Integrity, and Fraud Detection and Prevention.

References

[1] H. Alzoubi, M. Alshurideh, B. A. Kurdi, K. Alhyasat, and T. Ghazal, "The effect of e-payment and online shopping on sales growth: Evidence from banking industry," *Int. J. Data Netw. Sci.*, vol. 6, no. 4, pp. 1369–1380 (2022).

[2] S. Fatonah, A. Yulandari, and F. W. Wibowo, "A review of e-payment system in e-commerce," in *J. Phys.: Conf. Ser.*, vol. 1140, no. 1, p. 012033, IOP Publishing (2018).

[3] S. Firdous and R. Farooqi, "Impact of internet banking service quality on customer satisfaction," *J. Internet Bank. Commer.*, vol. 22, no. 1 (2017).

[4] K. Gupta and N. Arora, "Investigating consumer intention to accept mobile payment systems through unified theory of acceptance model: An Indian perspective," *South Asian J. Bus. Stud.*, vol. 9, no. 1, pp. 88–114 (2020).

[5] A. Kumar, A. Adlakaha, and K. Mukherjee, "The effect of perceived security and grievance redressal on continuance intention to use M-wallets in a developing country," *Int. J. Bank Mark.*, vol. 36, no. 7, pp. 1170–1189 (2018).

[6] R. Gaba and D. Sharma, "Examining the impact of sustainable practices on bank's financial performance," *J. Inf. Optim. Sci.*, vol. 45, no. 8, pp. 2443–2457 (2024), doi: 10.47974/JIOS-1986.

[7] M. Sinha, H. Majra, J. Hutchins, and R. Saxena, "Mobile payments in India: the privacy factor," *Int. J. Bank Mark.*, vol. 37, no. 1, pp. 192–209 (2019).

[8] S. Singh and R. K. Srivastava, "Predicting the intention to use mobile banking in India," *Int. J. Bank Mark.*, vol. 36, no. 2, pp. 357–378 (2018).

[9] L. K. Dhillon, "Using AHP model to evaluate factor influencing mobile banking usage in Indian banks," *J. Stat. Manag. Syst.*, vol. 26, no. 5, pp. 1005–1014 (2023), doi: 10.47974/JSMS-1153.

[10] B. Sivathanu, "Adoption of digital payment systems in the era of demonetization in India: An empirical study," *J. Sci. Technol. Policy Manag.*, vol. 10, no. 1, pp. 143–177 (2019).

Received March, 2024