Educational Administration: Theory and Practice
2023,29(4) 3532 - 3536
ISSN:2148-2403
https://kuey.net/

Research Article

Combatting Security Issues In Digital Financial Services: A Banking Perspective

Rajagopal M[1*], Dr. K. Saravanan[2]

[1*]Ph.D Research Scholar, Dept. of Business Administration, Annamalai University
[2]Assistant Professor, Dept. of Business Administration, Annamalai University, (Deputed at Government Arts College, Dharmapuri)

Citation: Rajagopal M. K, et al (2023), Combatting Security Issues In Digital Financial Services: A Banking Perspective, *Educational Administration: Theory and Practice, 29(4),* 3532 - 3536
Doi: 10.53555/kuey.v29i4.8164

ARTICLE INFO

ABSTRACT

In an era where digital financial services are integral to everyday life, ensuring the security of transactions and data has become paramount. The rapid evolution of technology has revolutionized the banking sector, offering unprecedented convenience and efficiency. However, this digital transformation also presents significant security challenges that banks must address to safeguard customer trust and financial integrity. The rapid digital transformation in the financial sector has brought about significant advancements, but it has also introduced a range of security challenges. Various studies have examined these issues from different perspectives, providing insights into effective strategies for enhancing security in digital financial services. In this article has dealt with the security issues involved in the digital financial service offered by banks.

Keywords: Digital finance – Banking Service – Security Issues in digital service

1. Introduction

Banks are investing heavily in robust security measures to protect transactions and data from potential threats. These measures are designed to create a secure environment where customers can conduct their financial activities with confidence. By employing advanced security protocols, banks aim to mitigate risks associated with cyber threats, fraud, and unauthorized access.

A cornerstone of these security measures is the implementation of multilevel authorization to access accounts. This includes the use of Personal Identification Numbers (PINs), One-Time Passwords (OTPs), and security questions. These layers of security ensure that even if one form of authentication is compromised, additional barriers prevent unauthorized access. This multifaceted approach significantly enhances the protection of customer accounts and sensitive information.

Another critical aspect of securing digital financial services is the responsible use of customers' personal information. Banks are committed to using this data solely for authorized purposes, in compliance with stringent privacy regulations. By doing so, they ensure that personal information is not exploited for malicious activities, thereby maintaining customer trust and loyalty.

To further bolster security, banks have implemented automatic logout mechanisms. In scenarios where there is connectivity loss or when an account remains idle for a certain period, the system automatically logs the user off. This precautionary measure prevents unauthorized access that could occur if a user forgets to log out or if their device is left unattended.

Banks also employ sophisticated monitoring systems to detect and respond to unusual transactions. These systems analyze transaction patterns in real-time and flag any anomalies that could indicate fraudulent activity. When such transactions are identified, the bank immediately contacts the customer to verify the legitimacy of the transaction. This proactive approach is crucial in preventing fraud and protecting customers' financial assets.

2. Reviews of Literature

A key focus in the literature is the implementation of robust security measures to protect customer data and transactions. Multilevel authorization mechanisms, including the use of PINs, OTPs, and security questions, are widely recognized as effective in preventing unauthorized access to accounts. These measures form the first line of defense against cyber threats by ensuring that only authenticated users can access sensitive financial information (**Anakpo, Xhate, & Mishi, 2023**).
The implementation of automatic logout features to protect accounts in case of inactivity or connectivity loss is another important security measure discussed. This functionality helps to prevent unauthorized access when devices are left unattended. Furthermore, the proactive monitoring of unusual transactions and immediate customer notifications are crucial for early detection and prevention of fraudulent activities. This real-time approach to security ensures that potential threats are addressed promptly, reducing the risk of financial loss (Future Business Journal, 2023).

3. Research Design and Sample

In the present study descriptive research design will be adopted. Descriptive research studies are those studies which are concerned with describing the characteristics and attitude of a particular individual, or a group.
This study focuses to South Tamilnadu Private Sector Banks' Problems and Prospects of Digital Financial Services. Convenience sampling technique is applied to this study because to measure customers' opinion and perception of Problems and Prospects of Digital Financial Services. 757 Data were collected from potential respondents to understand specific attributes and opinions of Problems and Prospects of Digital Financial Services. Convenience sampling is a non-probability sampling method where units are selected for inclusion in the sample because they are the suitable for the researcher to access. This can be due to geographical proximity, availability at a given time, or willingness to participate in the research.

4. Objective of the study: to evaluate the prospects of digital financial services of various security measures on user trust and adoption.

5. Analysis and Interpretation

Path Regression Analysis of Digital Financial Service Prospects in Security Abbreviation of Security

Abbreviation	Security (SEC)
SEC -1	Sufficient measures are being taken to make transactions/data secure/safe
SEC -2	It is secured with multilevel authorization to access account which prevents unauthorized access (Pin / OTP / Security questions etc.)
SEC -3	Customers' personal information are used only for authorized purposes
SEC -4	In case of connectivity loss or account remaining idle for some time account automatically gets logged off
SEC -5	In case of unusual transaction bank contacts me immediately

Table- 1. Model Fit Summary

Model	R	R-Square	Adjusted R-Square	Std. Error of the Estimate	Durbin-Watson
Security	0.878	0.770	0.768	0.28662	2.051

Dependent Variable: Security

The model reveals that the R value (Multiple Correlation Coefficient) is 0.878, indicating a strong relationship between the prospects of digital financial service security and the predicted values. These predicted values include: 'Sufficient measures are being taken to make transactions/data secure/safe' (SEC-1), 'It is secured with multilevel authorization to access accounts, which prevents unauthorized access (Pin/OTP/Security questions, etc.)' (SEC-2), 'Customers' personal information is used only for authorized purposes' (SEC-3), 'In case of connectivity loss or the account remaining idle for some time, the account automatically gets logged off' (SEC-4), and 'In case of unusual transactions, the bank contacts me immediately' (SEC-5).

The R-Square (Coefficient of Determination) value is 0.770, meaning that more than 77% of the variation in digital financial service security is explained by the variations in these independent variables (SEC-1 to SEC-5). The adjusted R-Square value is 0.768, which adjusts the statistic based on the number of independent variables in the model, ensuring the goodness-of-fit.
Furthermore, the Durbin-Watson (DW) statistic, which ranges from 0 to 4, indicates the presence of autocorrelation. A value between 0 and 2 suggests positive autocorrelation, while a value between 2 and 4 indicates negative autocorrelation. In this case, the DW statistic is 2.051, indicating slight negative autocorrelation, which is considered acceptable.

Table- 2 ANOVA

Security	Sum of Squares	df	Mean Square	F	Sig.
Regression	156.932	5	31.386	382.052	0.000
Residual	46.745	569	0.082		
Total	203.677	574			

Dependent Variable: Security

The *F*-ratio in the **ANOVA** table interprets the overall regression model, which is a normal fit for the data. The result of F (5,569) = 382.052 and 'p' value 0.000 is less than 0.05 ($p < 0.05$), the regression model is a good fit for the data; therefore, this model is a linear relationship between the dependent and independent variables.

Fig-1 Path Regression Analysis of Digital Financial Services Prospects in Security

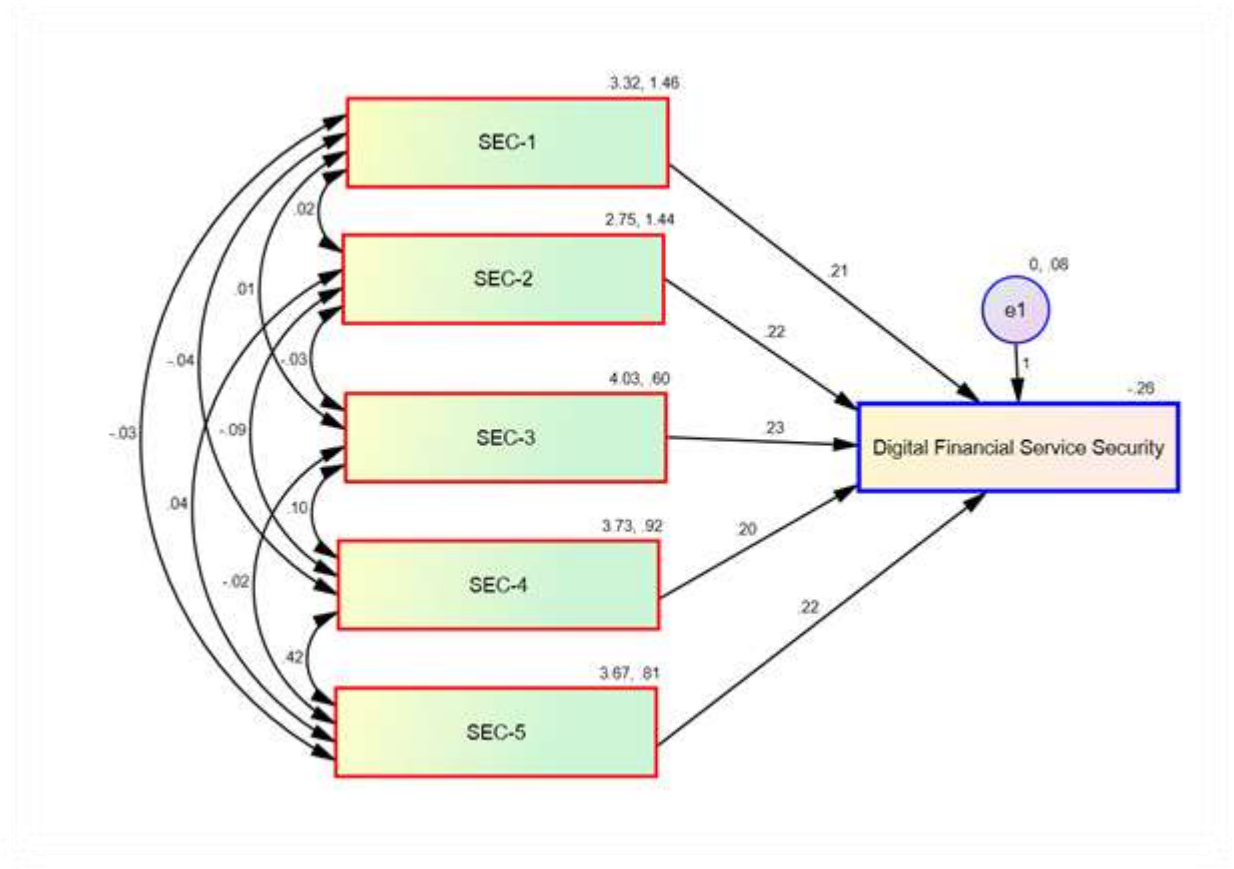

Table- 3 Regression Weights for Digital Financial Services Prospects in Security

Regression Weights	Estimate	S.E.	C.R.	P
Security <--- SEC-1	0.210	0.010	21.306	0.000
Security <--- SEC-2	0.217	0.010	21.786	0.000
Security <--- SEC-3	0.225	0.016	14.428	0.000
Security <--- SEC-4	0.199	0.014	13.762	0.000
Security <--- SEC-5	0.219	0.015	14.364	0.000

Note: .000 is 1% a -significant level

The path diagram illustrates the independent variables related to the prospects of digital financial services security, including: 'Sufficient measures are being taken to make transactions/data secure/safe' (SEC-1), 'It is secured with multilevel authorization to access the account, which prevents unauthorized access (Pin/OTP/Security questions, etc.)' (SEC-2), 'Customers' personal information is used only for authorized purposes' (SEC-3), 'In case of connectivity loss or the account remaining idle for some time, the account automatically gets logged off' (SEC-4), and 'In case of unusual transactions, the bank contacts me immediately' (SEC-5). Path regression analysis was applied to all five variables, and each was found to be highly significant at the 1% significance level.

Comparing the significant variables with their estimated values, the most influential variable for digital financial services prospects in security is 'Customers' personal information is used only for authorized purposes' (SEC-3) with an estimated value of 0.225. The second most influential variable is 'In case of unusual transactions, the bank contacts me immediately' (SEC-5) with an estimated value of 0.219. The third influential variable is 'It is secured with multilevel authorization to access the account, which prevents unauthorized access (Pin/OTP/Security questions, etc.)' (SEC-2) with an estimated value of 0.217.

The study concludes that the most critical aspects of digital financial services security are ensuring that customers' personal information is used only for authorized purposes and that banks promptly contact customers in case of unusual transactions.

6. Findings

1. Customers' Personal Information: The most influential factor in the security aspects of digital financial services is the assurance that customers' personal information is used only for authorized purposes. This variable (SEC-3) had the highest estimated value of 0.225, indicating its significant impact on users' perceptions of security.

2. Bank Response to Unusual Transactions: The second most influential factor is the bank's prompt response to unusual transactions. The variable 'In case of unusual transactions, the bank contacts me immediately' (SEC-5) had an estimated value of 0.219, highlighting the importance of real-time monitoring and communication in building trust and security.

3. Multilevel Authorization: The use of multilevel authorization to prevent unauthorized access (SEC-2) is another critical security aspect, with an estimated value of 0.217. This includes security measures like PINs, OTPs, and security questions, which significantly contribute to the overall security of digital financial services.

4. Transaction and Data Security Measures: The variable 'Sufficient measures are being taken to make transactions/data secure/safe' (SEC-1) is also significant, underscoring the importance of robust security protocols to protect transaction integrity and data privacy.

5. Automatic Logoff and Connectivity Loss: The security measure that logs off accounts automatically in case of connectivity loss or inactivity (SEC-4) is essential, though it had a slightly lower impact compared to the other factors.

7. Suggestions

Banks should prioritize and continually enhance data privacy protocols to ensure that customers' personal information is used solely for authorized purposes, supported by regular audits and transparency reports to maintain high standards. Implementing advanced systems for real-time monitoring of transactions and immediate communication with customers in case of unusual activity can significantly boost user confidence. Strengthening multilevel security measures, such as maintaining and upgrading PINs, OTPs, security questions, and incorporating biometric authentication, is essential for enhanced security. Continuous investment in advanced security technologies like encryption and blockchain, along with regular security updates and adherence to international standards, is crucial for robust transaction and data security. Additionally, optimizing automatic logoff features to prevent unauthorized access during connectivity loss or inactivity, while balancing security and user convenience with customizable inactivity periods, is necessary for effective protection.

8. Conclusion

The landscape of digital financial services is continuously evolving, and with it, the security measures needed to protect against emerging threats. Banks are at the forefront of this battle, implementing comprehensive security strategies to ensure that transactions and data remain safe. By focusing on multilevel authorization, responsible data use, automatic logout mechanisms, and proactive transaction monitoring, banks are committed to providing a secure and trustworthy environment for their customers. As the digital landscape continues to advance, these efforts will be essential in maintaining the integrity and reliability of financial services.

References:

1. Anakpo, G., Xhate, Z., & Mishi, S. (2023). The Policies, Practices, and Challenges of Digital Financial Inclusion for Sustainable Development. *MDPI*.
2. Future Business Journal. (2023). Unlocking the full potential of digital transformation in banking: a bibliometric review and emerging trend. *SpringerOpen*.
3. Yousafzai, S. Y., Pallister, J. G., & Foxall, G. R. (2003). A proposed model of e-trust for electronic banking. *Technovation*, 23(11), 847-860.
4. Shaikh, A. A., & Karjaluoto, H. (2015). Mobile banking adoption: A literature review. *Telematics and Informatics*, 32(1), 129-142.