Jurnal Manajemen Keuangan (MANKEU)
Vol. 3, No. 2, June 2025, hlm. 111~118
ISSN 2988-246X

THE INFLUENCE OF DIGITAL SECURITY SYSTEM RELIABILITY ON BANK BRI E-BANKING SERVICES

Lina Oktafiana[1], Ayu Sifriatul Imania[2], Ani Qotuz Zuhro' Fitriana[3]
[1,2,3]Da'wah Management Study Program, UIN Kiai Haji Achmad Siddiq Jember, East Java, Indonesia.
*e-mails: linaoktafiana2005@gmail.com

Article Info

Article history:

Received 06 04, 2025
Revised 06 09, 2025
Accepted 06 11, 2025

Keywords:

Digital security
E-Banking
BRI
Customer satisfaction

Abstract

This study aims to analyze the influence of digital security systems on the E-Banking services of Bank BRI. The advancement of digital technology facilitates financial transactions but also increases the potential for cybersecurity threats. Using a quantitative approach through the distribution of questionnaires to 30 student users of BRI E-Banking at UIN KHAS Jember, data were obtained regarding their perceptions of security and satisfaction with the BRIMO service. The research results show that the majority of respondents feel safe and satisfied with the implemented E-Banking system, with the percentage of "agree and strongly agree" responses exceeding 75% across various indicators. The validity test of the questionnaire shows that the instrument used is valid and relevant to measure the influence of digital security on e-banking services. This study emphasizes the importance of reliable digital security systems in maintaining customer trust and comfort in conducting electronic transactions.

1. INTRODUCTION

Background problem

Bank Rakyat Indonesia (BRI) is one of the banking institutions that is currently experiencing rapid development. As one of the largest state-owned banks in Indonesia, BRI operates conventionally but also has the potential to apply the principles of Islamic banking. Since its establishment in 1895, PT Bank Rakyat Indonesia (Persero) Tbk has remained committed to providing services to the lower classes. In addition to core banking activities, BRI also provides various additional services such as bill payments, online transactions, deposit acceptance services, BRIfast Remittance, and others. [1]

In the increasingly advanced digital era, the banking sector is experiencing very complex security challenges in online digital services. One of the main services that has experienced very rapid development is Electronic Banking (e-Banking), which makes it easier for customers to make transactions online through electronic devices. Bank Rakyat Indonesia (BRI), which is one of the largest banks in Indonesia and continues to develop e-Banking services to improve the convenience of financial services.

A service is an action or appearance that can be offered by one party to another party that is not in physical form and does not result in ownership rights. This service may or may not be related to a physical product. Service is an important factor in determining the success of various types of businesses engaged in the service sector. The role of service will be even more vital when competition in the service industry is quite tight, where companies strive to capture and maintain market share or customers. In a situation of intense competition, companies must be able to provide quality service to maintain the loyalty of existing customers. In general, service according to Purwadarminta is an effort to provide everything that is needed by others.

E-Banking services are inseparable from digital security risks. Cyber attacks, such as phishing, scamming, and other forms of cyber attacks, are increasing, making system and user vulnerabilities a target. Cases of digital attacks on the banking sector have experienced significant financial losses, reduced customer trust, and raised questions about the reliability of the bank's digital security system, including BRI.

Table 1: Financial Loss Data of Banking Sector 2021-2024

Year	Estimated Loss (IDR)
2021	± IDR 200 Billion
2022	± IDR 250 Billion
2023	± IDR 300 Billion
2024	± IDR 350 Billion

Source: (OJK Report, 2025)

Referring to the data above, losses continue to increase by 50 billion each year due to cyber attacks on E-Banking. This indicates that it is important to strengthen the reliability of the digital security system in e-Banking services. Customer trust in e-Banking services is highly dependent on their response to the digital security offered by the Bank. [2]

Problem Formulation

The problem that is the focus of this research is whether the reliability of the digital security system affects Bank BRI's e-banking services.

Research purposes

The purpose of this research is to conduct further research on the Influence of the Reliability of the Digital Security System on Bank BRI's E-Banking services.

2. LITERATURE REVIEW

Reliability

Reliability can be interpreted as the possibility of a system or its components being able to perform a predetermined function consistently, under certain operational conditions and for a predetermined period. This

reliability is generally measured using a probabilistic approach through the reliability function. In addition, other measures that are also used in assessing the reliability of a system include the failure rate (λ) and the mean time between failures (MTBF), which provide an idea of how often the system experiences disruptions. [3]

According to Tjiptono, reliability in the context of service reflects the extent to which customers can trust the quality of the service provided. This is reflected in the consistency of service without discrimination against customers and the accuracy of the service received according to expectations. Reliability is an important indicator in building customer trust and satisfaction with a company or service provider. [4]

Reliability in digital systems refers to the ability of a system to function stably, free from disruption, and remain optimal even when facing unexpected conditions. In this case, reliability is an important aspect, especially because users expect services that are always available and error-free, especially when dealing with important financial transactions that require a fast response. A system that can be accessed at any time, responds quickly, and provides accurate results will increase user confidence in the platform. This is in line with the reliability indicators put forward by Tjiptono, where consistency and accuracy are the main keys to creating customer satisfaction. Well-maintained reliability will strengthen the perception of behavioral control within the Theory of Planned Behavior (TPB) framework, because users feel able to control and predict the results of using the technology, thus further encouraging their intention to continue using fintech services. In its implementation in fintech services, system reliability includes technical aspects such as minimal digital interference, including phishing, scamming, and cyber attacks, that are closely related to user perceptions of the quality of service they receive.

The term "phishing" was first known in 1996 and is believed to originate from a play on words between "fishing" and an attempt to "fish for information" from victims. Phishing is also often referred to by other terms, such as brand spoofing or carding. The basic concept is similar to fishing, where the attacker spreads "bait" in the hope that most people will ignore it, but some are eventually "hooked" and provide their personal information. Felten and colleagues explain that spoofing is a technique used to gain illegal access to computers or information, in which the perpetrator disguises himself as a party trusted by the victim to deceive them. [5]

Phishing is usually done through email, text messages, or fake websites designed to look like legitimate services, such as banks or e-commerce platforms. The goal is to trick users into providing important information such as passwords, credit card numbers, or other personal data. This threat is increasingly dangerous because the methods used by perpetrators are increasingly sophisticated, often difficult to distinguish from official communications. In the book Fraud and Scam in the Digital Era: Concepts and Developments, scamming is explained as a form of fraud that is carried out systematically and deliberately to obtain personal gain, either in the form of money or sensitive personal data. This practice is usually carried out by fraudulent and deceptive methods. In the digital world, scamming includes various methods such as phishing, romance scams, fake investments, and fraud in online buying and selling transactions. Scammers, or scammers, often pretend to be trustworthy parties to trick victims into providing personal information or sending money. [6]

According to R. Suandhi, fraud is an act committed by someone by using trickery, a series of lies, false identities, or creating circumstances that do not by reality, to obtain personal gain illegally. What is meant by a series of lies is a collection of false statements that are arranged convincingly, so that it appears like a story that seems real. [7]

The term "cyber" comes from the word "cybernetics", which is a branch of science that studies how systems work automatically, including a combination of the fields of robotics, mathematics, electronics, and psychology. This science was first introduced by Norbert Wiener in 1948. From this word, then emerged the term cybercrime, which means a crime involving computers, internet networks, or other digital technology. Cybercrime can be a crime that attacks public systems on the internet or attacks someone's data or information. [8]

As digital technology develops, the forms of cybercrime are increasingly diverse, ranging from hacking, identity theft, spreading viruses, to online fraud (scamming). These crimes can have a major impact, not only economically but also on the security and privacy of users. Therefore, it is important for every internet user to

understand cyber threats and take preventive measures, such as using strong passwords, not sharing personal information carelessly, and installing adequate security software.

Layanan

Service is an action or performance that can be offered by one party to another party that is not in physical form and does not result in ownership rights. This service may or may not be related to a physical product. [9]

Service is an important factor in determining the success of various types of businesses engaged in the service sector. The role of service will be increasingly vital when competition in the service industry is quite tight, where companies strive to capture and maintain market share or customers. In a situation of intense competition, companies must be able to provide quality service to maintain the loyalty of existing customers. In general, service according to Purwadarminta is an effort to provide everything that is needed by others. [10]

Previous Research

In line with this research, Munthe et al. explained that reliability in digital systems causes customer constraints in using E-Banking services and the speed and responsiveness of the E-Banking service network/site, so that it will later affect customer satisfaction in using it. [11]

Research by Anggun et al., which discusses the Influence of Service Quality, Perception of Usefulness and E-Banking on BRI Bank Customer Satisfaction, also shows that customer satisfaction can be achieved through good and reliable e-Banking services. Good services include systems that allow customers, both individuals and business actors, to access accounts, conduct various financial transactions, and obtain information related to bank products and services through private and public networks, including the internet, safely and accurately.

3. RESEARCH METHOD

This study uses a quantitative approach with a quantitative descriptive research type. This approach was chosen to measure the influence of the digital security system on the quality of BRI Bank E-Banking services based on numerical data from the questionnaire results.

The data collection method was carried out by distributing closed questionnaires based on Google Forms to 30 respondents who were students who used BRI E-Banking services at UIN KHAS Jember. The sampling technique used was purposive sampling with the criteria of active users of the BRIMO application. This data is used to explore information about the influence of the reliability of the digital security system on BRI Bank E-Banking services. In this study, the type of data used was the results of the questionnaire, so that participants could interpret the experience gained. The preparation of questionnaire statements used the theory of DeLone and McLean, which reviewed information systems from digital system security, experience using E-Banking, customer trust, and satisfaction to measure the effectiveness of Google Forms. Furthermore, the sample was determined by purposive sampling with the criteria: BRI Bank E-Banking users who were taken evenly from all faculties.

The validity of the instrument was tested using the Pearson Product-Moment correlation, while reliability was tested using Cronbach's Alpha. The results of the reliability test showed an alpha value of 0.83, which means that the instrument has high internal consistency and can be used reliably.

To find out how much influence the digital security system has on E-Banking services, simple linear regression is also used. This regression is carried out by setting the digital security system as a variable (X) and satisfaction with E-Banking services as a variable (Y). The results of this simple linear regression are used to determine the extent of the security system's contribution to changes in service satisfaction.

The data collection technique was carried out using a questionnaire (Google Form) to E-Banking users in the sample. The type of questionnaire used in this study is a closed questionnaire or structured questionnaire (Closed Questionnaire). According to Djaali, "a closed questionnaire is a questionnaire whose alternative answers

have been provided, and respondents, questionnaires distributed online using a Likert scale are used to measure". The Likert scale, according to Priyono, concerns systematic statements to show the scale of a respondent's attitude towards the statement. And asked to choose one answer that matches the characteristics of the questionnaire. The questionnaire consists of two parts using a Likert scale: 1. Strongly Disagree, 2. Disagree, 3. Agree, 4. Strongly agree.
The data is presented in the following criteria ranking groups:

Table 2: Rating Criteria

Criteria	*Rating*
If the average number of respondents' answers is "Agree and Strongly agree," then the digital reliability system has a strong influence on service	++
If the average number of respondents' answers is "Strongly Disagree and Disagree," then the digital reliability system has a weak influence on service +	+

4. RESULTS AND DISCUSSION

Referring to the respondent criteria in this study, the questionnaire was then distributed for three months of the study period. All maximum efforts were made to convince respondents to respond to the instrument with quick and appropriate responses regarding each item. The questionnaire was used as a measure of the security of the E-Banking digital system for customer trust and satisfaction.

The results of the data collected showed that the digital security system has a significant influence on BRI Bank's E-Banking services. This is evidenced by the percentage of 'agree', which is greater than other Likert scales, which is 904.8%. In the results of this study, customers who use E-Banking on average trust and are satisfied with BRI Bank's E-banking services. The presentation of this data can be seen in the following table.

Respondent responses have been evenly distributed to all types of business units, so that they are expected to be able to provide a comprehensive picture of information in answering the formulation of the problem in this study. The results obtained by the UIN Khas Jember student questionnaire, the percentage of the STS Likert scale with a percentage of 105.1%, the percentage of the TS Likert scale with a percentage of 121.2%, the percentage of the S Likert scale with a percentage of 904.8%, and the percentage of the SS Likert scale with a percentage of 415.9%. At the level of effectiveness of the Google form, measured based on the influence of the digital security system on BRI Bank E-Banking services, the lowest score obtained was 105.1%.

Validity Test

The validity test was conducted to measure whether the questionnaire instrument was truly able to measure the variables studied, namely the effect of digital security system reliability on E-Banking services. The technique used was Pearson's product-moment correlation. The following are the results of the validity test on 10 random questions from the questionnaire:

Table 3: Validity test results

Statement	r count	r Table (n=30; α=0,05)	Note
Security of E-Banking transactions	0,765	0,361	Valid
Confidence in the BRIMO security system	0,711	0,361	Valid
Concerns about fraud by the BRIMO application	0,693	0,361	Valid
BRI routinely updates its security system	0,730	0,361	Valid
Personal data is protected in E-Banking	0,689	0,361	Valid
Convenience in transactions	0,754	0,361	Valid
Direct transaction notifications	0,641	0,361	Valid

Transactions are recorded correctly	0,672	0,361	Valid
The BRIMO application is easy to use	0,798	0,361	Valid
Security is the main reason to continue using E-Banking	0,723	0,361	Valid

If the calculated r value > r table (0.361), then the question item is categorized as valid. From the table above, all items have a significant correlation, so all items are considered suitable for use in research.

Reliability Test (Cronbach's Alpha)

To determine whether the questionnaire instrument is consistent and reliable, a reliability test is carried out using the Cronbach's Alpha formula. The calculation results are shown in the following table:

Table 4: Reliability test results

Statement	Item-Total Correlation	Note
Security in conducting E-Banking transactions	0,712	Reliabel
Confidence in the BRIMO security system	0,694	Reliabel
Concerns about fraud by the BRIMO application	0,652	Reliabel
BRI routinely updates its security system	0,721	Reliabel
Personal data is protected in E-Banking	0,668	Reliabel
Convenience in making transactions	0,735	Reliabel
Direct transaction notifications	0,670	Reliabel
Transactions are recorded correctly	0,688	Reliabel
The BRIMO application is easy to use	0,745	Reliabel
Security is the main reason to continue using E-Banking	0,7699	Reliabel
Cronbach's Alpha Total	**0,819**	**Reliabel**

The Cronbach's Alpha value of 0.819 > 0.7 indicates that the instrument has high reliability, so that all statement items are suitable for use in research.

Normality Test (Shapiro-Wilk)

Because the number of samples is 30 (n < 50), the Shapiro-Wilk test is used to determine whether the data is normally distributed. The test results are presented in the following table:

Table 5: Normality Test (Shapiro-Wilk)

Variabel	Statistics W	Sig. (p-value)	Data Distribution
Perception of Digital Security System	0.972	0.316	Normal
User Satisfaction with Services	0.968	0.289	Normal

Because the Sig. value > 0.05, the data is declared normally distributed and meets the requirements for parametric analysis.

Correlation Analysis

Correlation analysis is used to determine the relationship between Digital security reliability (X) and BRI Bank E-Banking Services (Y).

Table 6: Pearson Product-Moment Correlation Test Results

Variable	X	Y
Digital security reliability (X)	1,000	0.723**
BRI Bank E-Banking Services (Y)	0,723**	1,000

The R value = 0.723 indicates a strong positive relationship between digital security and customer satisfaction.

(**): Significant correlation at α = 0.01.

Simple Linear Regression Analysis

To find out how much influence digital security (X) has on customer satisfaction (Y), a simple linear regression model is used:

$$Y=a+bXY = a + bXY=a+bX$$

Coefficient	Value	Note
Intersep (a)	12.45	Constant
Koefisien (b)	0.68	Positive influence on Y
R	0.723	Correlation coefficient
R Square (R^2)	0.523	Contribution of variable X to Y: 52.3%
Sig. (p-value)	0.000	Significant at α = 0.05

Regression Equation:

$$Y=12.45+0.68XY = 12.45 + 0.68XY$$

- The R value = 0.723 indicates a strong and positive relationship between the digital security system and customer satisfaction.
- R^2 value = 0.523 means that 52.3% of the variation in customer satisfaction can be explained by digital security, while the rest (47.7%) is explained by other factors.
- The significance value (p = 0.000) shows that the relationship is statistically significant.

Based on the results of the correlation and regression analysis, the digital security system has a strong and significant effect on customer satisfaction with BRI Bank's E-Banking services. The higher the perception of digital security, the higher the level of satisfaction felt by customers.

5. CONCLUSION

This study concludes that the digital security system has a significant influence on the quality of BRI Bank's E-Banking services, especially through the BRIMO application. This is reflected in the results of the questionnaire, where the majority of respondents felt safe, comfortable, and satisfied when using E-Banking services. The data shows that a reliable digital security system can increase customer trust and encourage the intensity of service use.

6. SUGGESTION

It is recommended that Bank BRI continue to develop and update its digital security system regularly and educate customers regarding online transaction security. In addition, further research with a larger sample size and a mixed-methods approach can provide more comprehensive results.

BIBLIOGRAPHY

[1] Permana, I. S., Halim, R. C., Nenti, S., & Zein, R. N. (2022). "Analisis Kinerja Keuangan Dengan Menggunakan Rasio Likuiditas, Solvabilitas dan Profitabilitas Pada PT. Bank BNI (Persero), TBK." *Jurnal Aktiva : Riset Akuntansi dan Keuangan* 4, no. 1.

[2] Muhammad. V. F. (2024). "*Cyber Crime terhadap loyalitas nasabah dengan kepercayaan sebagai variable Intervening (studi pada nasabah Bank Syariah di Kota Bandar Lampung)".* Skripsi, Universitas Islam Negeri Raden Intan Lampung.

[3] Ebeling, C.E. (1997). *An Introduction to Reliability and Maintainability Engineering.* Singapore: McGraw-Hill.

[4] Fandi, Tjiptono (2014). *Pelayanan, Kualitas & Kepuasan*. Edisi 3. Yogyakarta: Penerbit Andi.

[5] D. Dean, E. W. Felten, and D. S. (1996). *Wallach. Java security: From HotJava to Netscape and beyond. In Proceedings of the 1996 IEEE Symposium on Security and Privacy*.

[6] Hopkins, A. (2015). *Scamming 101: 22 scams explained*. Amazon Digital Services.
[7] Sugandhi, R. (1980)., Kitab *Undang-undang Hukum Pidana dan Penjelasannya*, Usaha Nasional, Surabaya.
[8] Kurniawan, R. (2019). *Kejahatan Dunia Maya: Teori dan Studi Kasus Cybercrime*. Jakarta: Prenadamedia Group.
[9] Kotler (1999). *Marketing Management: An Asian Perspective*. Prenhallindo.
[10] Purwadarminta (1996). *Kamus Umum Bahasa Indonesia*. Balai Pustaka.
[11] Munthe, Surya D., dan Inggrita GS Nasution (2013). "Survei Kepuasan Konsumen terhadap Pemanfaatan Layanan E-Banking pada Bank-bank Umum di Kota Medan." *Jurnal Ekonomi dan Keuangan* 1, no. 12.