Journal of Theoretical and Applied Information Technology
15th November 2022. Vol.100. No 21

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ANALYSIS OF FACTORS AFFECTING FIN-TECH FORENSIC ON APPLICATION OF QRIS IN PAYMENT SYSTEM

[1]ARYANTI WARDAYA PUSPOKUSUMO, Management Department, Binus Business School,
Bina Nusantara University, Jakarta, Indonesia, 11480.
[2]BAMBANG LEO HANDOKO, Accounting Department, School of Accounting,
Bina Nusantara University, Jakarta, Indonesia, 11480.
E-mail: [1]rpuspokusumo@binus.edu, [2]bambang.handoko@binus.edu.

ABSTRACT

Disruption of the use of financial technology is undoubtedly unavoidable. One of the pieces of evidence is developing the primary business model of financial technology, specifically digital payments. Various applications offer convenience in making payments, applying the QR code scan payment method. The variety of QR Codes provided by the application is why Bank Indonesia standardizes the QR Code into QRIS (QR Code Indonesian Standard). Behind the good hopes at digital payment services, of course, it cannot be denied that the development of cybercrime is also increasing. Fin-tech Forensics, a combination of fin-tech and digital forensics science, aims to investigate and reconstruct criminal financial activities. Our research want to test effects implementation of QRIS on fin-tech forensics in Jakarta using indicators based on previous literature studies. The method used in data collection is by distributing questionnaires. All data were processed using Smart PLS 3. This study indicates that two variables perceived guardianship and perceived cyber threats each has significant and positive effect on fin-tech forensics. On the other hand, security and trust not significantly affects fin-tech forensics on application of QRIS in payment system.

Keywords: *Digital, Payment, Cybercrime, Fin-tech, QRIS, Forensic.*

1 INTRODUCTION

1.1 Research Background

Financial Technology or better known as fin-tech is a one of the innovations that are influenced by technological advances. Fin-tech that can be indicated as the use of technology to provide solutions in finance services for customers [1] plays a role as disruption and introduces a new concept in financial services that increases global awareness in this industry. In its development to facilitate e-wallet-based transactions, the method of execution of the digital payment has also developed. One of which is use of Quick Response Code or QR Code. Each service provider Digital wallets are also competing to provide a QR Code for each one application. This of course causes disruption for both consumers and consumers merchants [2]. Seeing this phenomenon, Bank Indonesia launched QR Code standard known as QR Code Indonesian Standard (QRIS).

On the other hand, development regardless of what it is, will have an impact both positive and negative, the same thing happened to the development of fin-tech. The development of society is directly proportional to the development of crime in Indonesia society allows the emergence of new fraud opportunities can be threatens fin-tech users, it is this phenomenon that drives Bruce Nikkel carries the term fin-tech forensics. This term combines two aspects namely fin-tech and digital forensic science, so that fin-tech forensics can be defined as the application of digital forensic science to financial technology for the purpose of investigating and reconstructing criminal financial activity [3].

In Indonesia itself, crime in the fin-tech world cannot be categorized as a little. Based on data from the National Cyber and Crypto Agency (BSSN), throughout the month January to August 2020, there were nearly 190 million cyber-attack attempts on Indonesia, increased more than four times compared to the same period last year recorded in the range of 39 million. The highest number was recorded in August 2020, where BSSN recorded the number of cyber-attacks in the range of 63 million, much higher than August 2019 which was only in the range of 5 million [4].

Another well-known case is the case of the Central Bank of Bangladesh which hacked by hackers, where hackers use malware to infiltrate the

Central Bank of Bangladesh, then the hacker did impersonation and doing money laundering in casinos [5]. Based on the explanation above, these phenomena form the basis for this research.

1.2 Problem Statement

Problem statement in this research is as follow:

1. Does perceived cyber threat has significance effect on Application of QRIS payment system?
2. Does security and trust has significance effect on Application of QRIS payment system?
3. Does perceived guardianship has significance effect on application of QRIS payment system

2 LITERATURE REVIEW

2.1 Fin-Tech

Technological developments, various innovations were born to facilitate human relations, one of which is financial technology, or simply "fin-tech". Along with rapid digitalization acceleration and the growth of start-up companies, the greater the acceleration of fin-tech to be accepted by the wider community. Indonesian fin-tech technology started in 2006 [6].

Acceleration of widely known fin-tech brings many good impacts. The benefits of fin-tech are as follows: easier financial transactions, better access to funding, increasing people's living standards, supporting financial inclusion, accelerating economic turnover. It also has resulted in the emergence various fin-tech product innovations that help financial activities and support people's lives. The following are the types of fin-tech that have developed recently: peer to peer lending, crowd funding, e-wallet, micro finance, payment gateways, investments, digital banks.

2.2 Fin-Tech Forensic

The term fin-tech forensics is a combination of fin-tech and digital forensics science. Fin-tech forensics can be defined as the application of digital forensic science to financial technology for the purpose of investigating and reconstructing criminal financial activity. The discipline of digital forensics covers many different fields including computer forensics, network forensics, mobile forensics, malware forensics, Internet of Thing forensics, drone and vehicle forensics, and so on [3].

Cyber-criminal activities involving financial transactions can have several scenarios such as: presence of victims of crime (theft or extortion of funds), the existence of criminal up to criminal transactions, and crime against internet user [7].

Investigations of cyber fraud and other technical manipulations of financial systems typically involve understanding and reconstructing criminal activity, linking people or organizations involved in crimes, and finally collecting and preserving digital evidence. A comprehensive technical understanding of financial technology will enhance each of these phases. This technical analysis should support or be in line with existing investigative activities, such as accounting and forensic audits, AML investigations, and traditional fraud and crime investigations. Fin-tech forensic investigation and analysis should be complementary [3].

2.3 Effect of Perceived Cyber Threat on Fin-tech Forensic on Application of QRIS Payment System

Perceived security risk can be interpreted as the potential for loss of privacy and security personal information for the use of a product. The problem of security of personal data and accounts is one of the main contributing factors people refuse to use QRIS.

According to [8] in their research, it is revealed that trust affects perceptions of usefulness in fin-tech adoption but this does not affect service use but on the other hand, conceptual studies conducted by [9] shows that knowledge about perceptions of identity theft, perceptions of impersonation, and accounts that are considered hijacked are perceived as cyber security threats from the customer's point of view can hinder adoption and retention of e-banking adoption as well as generate skepticism, and a sense of reluctance to engage or maintain a transaction space [9]. So based on the results of these two studies, the hypotheses to be proven in this study are as follows.

H1: Perceived cyber threats have a significant positive effect on fin-tech forensics on the implementation of QRIS in payment system

2.4 Effect of Security and Trust on Fin-tech Forensic on Application of QRIS Payment System

Security and trust refers to whether users feel that using the QRIS payment application is safe or not. Users believe it or not to the seller who installs the QRIS code at the merchant. If the user trusts the merchant, the user will not hesitate to use QRIS for payment. QRIS payments are more effective because they are cashless, especially in the Covid-19 pandemic era which avoids paying cash.

On the other hand, [10] in their research revealed that an increase in the number of interfaces in fin-tech implementation will continue to increase the chances of cyber-security risks. [11] revealed that the implementation of strong and effective cyber security risk management controls can protect the fin-tech banking system from cyber-attacks [12]. By analyzing the results of the study and taking the CIA Triad approach, which is the core principle of information security, there are hypotheses to be proven in this study.

H2: Security and trust has a significant positive effect on fin-tech forensics on the implementation of QRIS in payment system

2.5 Effect of Perceived Guardianship on Fin-tech Forensic on Application of QRIS Payment System

People want to use the QRIS payment system if they feel that someone is protecting them. For example, there is money back balance protection if the account is broken into. One example is the Gopay application, which has a money back guarantee program if the account is hijacked.

[13] state that most criminal acts require convergence in time and space, a possible perpetrator, a suitable target, and the absence of a guardian capable of fighting crime [14]. Responding to these findings, by focusing on the guardianship factor, Elyas et. al. revealed that one of the factors that contribute to digital forensics readiness is policy [15], similar result found in [16] on guardianship through the ITE Law as a strategy to prevent cybercrime. Run by the government in its formal role shows that there is urgency for the trust itself [16]. Based on the results of this study, the hypotheses to be proven in this study are as follows.

H3: Perceived Guardianship has a significant positive effect on fin-tech forensics on the implementation of QRIS in payment system

3 RESEARCH METHODOLOGY

We conducted quantitative research methodology in this study. We used statistical tests to test the hypotheses presented in chapter 2. The population in this study which can later be concluded is QRIS users who are domiciled in Jakarta. The population of QRIS users domiciled in Jakarta is 3,331,429 people based on population census data conducted by the Central Statistics Agency [17]. We chose respondents who use QRIS in Jakarta because the most QRIS users in Indonesia are in Jakarta, which is the capital city, the most populous and the most advanced information technology.

The sample technique approach is utilized in this research about is employing a sample of non-probability. The use of this technique is due to the unequal opportunity for members of the population to be used as research samples. The sample is part of the number and characteristics possessed by the population. Based on the population that has been described previously, the number of samples needed so that it can accommodate Slovin Formula [18]: n = N/Ne2 + 1. With a 90% confidence level, the error tolerance limit is 10%, so the sample calculation is as follows: n = 3,331,429/(3,331,429)(0.1)2 + 1 = 101 sample respondents.

Data analysis in this study is using structural equation modelling. According to [19], Structural Equation Modelling is a modelling technique that allows a separate relationship for each set of independent variables. The Partial Least Square (PLS) approach is an alternative estimation approach for Structural Equation Modelling (SEM) where the results of factor analysis are represented in the composite in the construction of the study, without any attempt to recreate the covariance between the items measured [20].

In the field of information systems, the PLS-SEM technique is the most frequently used technique. The use of this technique is due to the assumption that PLS-SEM is a universal and most developed system [21]. The field of information systems has also been identified as the main user of PLS for analysing and testing theoretical propositions. In addition, the PLS-SEM technique itself is used for confirmation and exploration purposes.

Our research uses latent variables, in order to make the latent variables measurable, so we make operationalization variables.

Variable operationalization is presented in Table 1 below:

Table 1 Operation of Variables

Operation of Variables		
Variable	**Main indicator**	**Source**
Perceived Cyber Threat (PCT)	*1. Awareness of the importance of personal data* *2. Personal data security on the server* *3. Recorded personal data is difficult to steal*	[9]

Operation of Variables		
Variable	**Main indicator**	**Source**
	4. There is authorization for activities *5. The existence of authentication of activities* *6. Periodically update the password* *7. Awareness of grammar errors* *8. Awareness of visceral triggers* *9. Awareness of the return address*	
Security and Trust (ST)	*1. There is a request for permission to access data* *2. The existence of communication channels that are specifically created to increase confidentiality* *3. Encrypted communication channel* *4. Unable to retrieve information from recycled media or discarded media* *5. Permission to disclose confidential information* *6. There are limitations on computing devices/systems* *7. There is a control mechanism between actors/transactions* *8. 24/7 service availability* *9. Minimum number of service interruptions* *10. In case of interruption, service interruption duration is short*	[11]
Perceived Guardians (PG)	*1. There are rules for using the internet* *2. There are monitoring actions carried out* *3. Intervention behavior is carried out if there is a possibility of a crime* *4. There is clear legal protection*	[13]
Fin-tech Forensic (FF)	*1. Minimize case waiting time* *2. Maximizing the coverage of digital data/materials* *3. Efficient mobilization*	[3]

4 RESEARCH RESULT

4.1 Overview of Respondents

In this study, a questionnaire was used to collect data from the respondents. The questionnaire was compiled using Microsoft Form and the results were downloaded in the form of an excel file. The questionnaire was distributed to respondents who have used fin-tech payment systems, especially QRIS users and are domiciled in Jakarta. The number of respondents obtained is as many as 125 respondents

Table 2 Identity of Respondent

	Gender		Education
Male	46	High School	35
Female	79	Bachelor	77
	Age	Master	13
30 years <	51	Job:	
31-40 years	39	Student	54
41-50 years	23	Employee	57
> 50 years	12	Business	14

According to Table 2, most of our respondent are female, ages under 30 years old, work as employee and has educational level of bachelor.

4.2 Validity Test using Outer Loading

The results of the convergent factor loading validity test will be conducted through refers to outer loading value on indicators from each variable. In the convergent validity test the factor loading will show the correlation between the indicator and the construct. Where when the indicator with a low loading value indicates that the indicator does not work on the measurement model. Based on the number of samples as many as 125 samples, according to [22], the expected loading factor value is greater than 0.5 [22]. Table 3 show the result from outer loading test, after we outliers some indicators which has value under 0.5, finally we have indicators which has outer loading value more than 0.5

Table 3 Outer Loading Value

Indicator	Loading	Indicator	Loading
PCT2	0.690	I4	0.735
PCT3	0.663	A3	0.598
PCT4	0.510	G1	0.609
PCT5	0.670	G2	0.732
PCT6	0.739	G3	0.808
C2	0.800	G4	0.732
C3	0.656	FF1	0.916
I1	0.653	FF2	0.901
I2	0.505	FF3	0.909
I3	0.696		

After the values of the six invalid indicators are removed, the loading factor value becomes valid with a value greater than 0.5.

4.3 Convergent Validity Test using AVE

The results of the Average Variance Extracted (AVE) convergent validity test will be carried out by looking at the Average Variance Extracted (AVE) value in each variable. [22] said an AVE value of 0.5 or greater indicates that constructs explain that more than half of the variance comes from the indicators, while the AVE value of less than 0.5 indicates more variance comes from errors or errors and not from the construct [22].

Table 4 presented the AVE result, which indicates that all variables each has AVE value more than 0.5:

Table 4 Average Variance Extracted

Variable	Average Variance Extracted (AVE)
Perceived Cyber Threats	0.634
Security and Trust	0.648
Perceived Guardianship	0.524
Fin-tech Forensic	0.826

4.4 Reliability Test

In their book, [23] states that the reliability test is carried out at the variable level. The reliability test is also known as internal consistency and can be done by looking at the value of Cronbach's Alpha and Composite Reliability.

If Composite Reliability and Cronbach's Alpha fall below 0.6 than it considered as poor [24]. Variables that have Cronbach's alpha and composite reliability values from 0.6 to 0.8 are considered good (reliable).

The result presented in Table 5.

Table 5 Reliability Test

Variable	Cronbach's Alpha	Composite Reliability
Perceived Cyber Threats	0.679	0.791
Security and Trust	0.796	0.848
Perceived Guardianship	0.692	0.863
Fin-tech Forensic	0.894	0.934

Based on the outcomes about Cronbach's alpha and composite reliability tests carried out on the collected information, it can be expressed that all factors meet the least criteria of 0.6 and it can be expressed that all factors can be valid.

4.5 Determination Coefficient Analysis

Changes within the R-square are utilized to clarify the impact of certain latent exogenous variables on the dependent latent variable whether it has a substantive effect [21]. The Determination Coefficient (R^2) shows the strength of the relationship among construct in this study. The Coefficient determination test is presented in Table 6.

Table 6 Coefficient of Determination

Variable	R Square	Adjusted R Square
Fin-tech Forensic	0.458	0.445

Based on table 6, it can be concluded that the effect of Perceived Cyber Threats, Security and Trust, and Perceived Guardianship on Fin-tech Forensics is 0.445. This can be interpreted that the ability to influence the variables Perceived Cyber Threats, Security and Trust, and Perceived Guardianship on the fin-tech forensics variable is 44.5% while 55.5% is explained by other factors outside of this study.

4.6 Path Coefficient Analysis

Path coefficient test is utilized to appear whether there's an impact between factors. In case the more prominent the esteem of the path coefficient on one variable to another, the more grounded the impact between these factors. To discover out whether the latent variable features a critical relationship or not, t-statistics or p-value are utilized. Agreeing to [23], the estimation will meet the prerequisites of concurrent legitimacy, with a factual esteem more noteworthy than the table esteem (t-statistic 1.98) and p-value <0.05, it can be concluded that all noteworthy markers degree the dependent variables [21].

Table 7 Path Coefficient Analysis

Path	Original Sample	T statistic	p-value sig.
PCT → FF	0.264	2.509	0.006
ST → FF	0.207	1.613	0.054
PG → FF	0.343	3.789	0.000

Based on the test results in table 7 on the entire sample above, it can be concluded that: Hypothesis 1 (H1): Perceived cyber threats have a significant positive effect on Fin-tech Forensics on the implementation of QRIS in the financial technology payment system in Jakarta. The path coefficient T-Statistics is 2.509 (≥1.98) with P-Values 0.006 (≤0.05).

Hypothesis 2 (H2): Security and trust does not have a significant effect on fin-tech forensics on the implementation of QRIS in the financial technology payment system in Jakarta. T statistic is 1.613 (≤1.98) with a P-Value of 0.054 (≥0.05).

Hypothesis 3 (H3): perceived guardianship has a significant positive effect on fin-tech forensics on the implementation of QRIS in the financial technology payment system in Jakarta. T statistic is 3.789 (≥1.98) with a P-Value of 0.000 (≤0.05).

Figure 1 presented the path coefficient and coefficient determination.

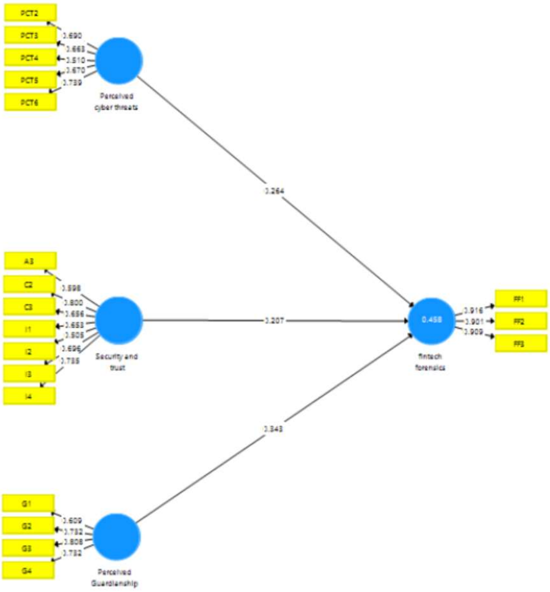

Figure 1 Research Path Coefficient

4.7 Discussion

The results of hypothesis testing that have been carried out show the effect of perceived cyber threats on fintech forensics. Bernik and Mesko conducted a study of the average internet user's knowledge accurately to examine perceptions of cybercrime and attempt to understand fears about it. The results of this study reveal that respondents have fairly good information about cybercrimes but only on crimes that are exposed in the media. Based on this study, it was also found that knowledge of cybercrime tends to increase the individual's fear of cybercrime. Users who are more aware of the risks in cyberspace and know how to deal with them are less likely to be afraid of becoming victims of cybercrime [25].

According to Atlam et.al, the insignificant relationship between security and trust in digital forensics can be caused by the heterogeneity of IoT devices, the adoption of one of the classical investigative frameworks will not be effective in digital investigations. The adoption of an IoT-based investigative framework is the main solution to this problem [26]. But on the other hand, computer forensics, which is a new discipline, still lacks standardization and consistency across courts and industry, so it has not been recognized as a formal scientific discipline.

Another study stated that a secure communication channel as an infrastructure for a digital forensic environment is something that needs attention, but unfortunately most digital forensics activities are currently carried out in a closed environment so that they have not utilized an interconnected system based on the availability of computer networks and the internet [27].

Khando et. al. in his research revealed that a number of negligence on the confidentiality, integrity, and availability of information system assets were caused by relying on technical solutions that were not contextually appropriate and adequate. According to Khando et. al. a large number of organizational information security incidents are caused by the exploitation of the human element that directly and/or indirectly causes these incidents. So that awareness of information security becomes one of the important aspects of protecting information security [28].

Perceived guardianship has a significant positive effect on fin-tech forensics on the implementation of QRIS in the payment system. The results obtained in this hypothesis are complementary to previous research conducted by [13]. In [13] conducted research related to the adoption of a digital forensic risk model that measures investigators' experience with eight important aspects of the digital forensic process. In this study, questions were asked about responses to the perceived risk of appropriate digital forensic procedures, handling/examination of evidence, acceptance, and other related issues of certain threats, as well as preventive measures that respondents can take to counter these threats. One of the results of the study stated that the minimization/mitigation of digital forensic risk will greatly facilitate the success of digital forensic investigations, ensuring that legal standards of evidence and acceptance are met.

5 CONCLUSION AND SUGGESTION

Result of this paper show that perceived cyber threats, and perceived guardianship have significance effect on the implementation of QRIS in the financial technology payment system in Jakarta. In contrary, security and trust does not has significance effect.

QR codes are evidence of developments in the field of digital payment technology. The phenomenon of the emergence of various QR codes from each application, led Bank Indonesia to the decision to integrate and standardize QR codes into QRIS. On the other hand, developments in the field of technology have also increased the development of cybercrime, especially for criminal tactics in which fintech technology is classified as high and cannot be ignored.

Therefore, this study will focus on the application of QRIS to fintech forensics, while also focusing on users who use the internet in DKI Jakarta. Based on the results obtained in this study in answering the objectives and formulation of research problems, it can be concluded that:

Perceived cyber threats, which is a level where measuring awareness or perception of the threat of crime has a significant positive effect on fintech forensics. This indicates that QRIS users are aware of the dangers of crime in fintech payment systems.

Security and trust in relation to the CIA Triad has a positive but not significant effect on fintech forensics. This insignificance is possible due to uncontrollable conditions.

Perceived guardianship is a level where measuring respondents' perceptions of reliable safeguards to protect and prevent crime has a significant positive effect on fintech forensics. Based on the results of data processing, the perceived guardianship variable is more influential than perceived cyber threats in relation to the implementation of QRIS in fintech forensics.

The suggestions for further research are as follows. The first suggestion is to add data that can expand the respondent's profile, such as expanding the scope of respondents, a more detailed specification of the type of work. The more information related to the respondent's profile, the deeper the ability to analyze the factors that affect fintech forensics in relation to the QRIS feature.

The second suggestion is to specify the target respondents for companies that provide digital payment systems services so that they get insight from the side of the company that provides services. By targeting respondents to digital payment systems service companies, future research can look at new aspects based on the developer's perspective on the implementation of QRIS in fintech forensics.

The third suggestion is to add variables that are considered relevant to the effect of implementing QRIS on fintech forensics in order to enrich the analysis results, such as technology culture and system architecture.

This paper limitation is only use 119 respondents from QRIS user in Jakarta. Further researcher hopefully will extend the area of research object.

REFERENCES

[1] A. Al-Okaily, M. Al-Okaily, F. Shiyyab, and W. Masadah, “Accounting information system effectiveness from an organizational perspective,” *Manag. Sci. Lett.*, vol. 10, no. 16, pp. 3991–4000, 2020, doi: 10.5267/j.msl.2020.7.010.

[2] C. Ellinas, “The Domino Effect: An Empirical Exposition of Systemic Risk Across Project Networks,” *Prod. Oper. Manag.*, vol. 28, no. 1, pp. 63–81, 2019, doi: 10.1111/poms.12890.

[3] B. J. Nikkel, “Fintech forensics: Criminal investigation and digital evidence in financial technologies,” *Digit. Investig.*, vol. 33, p. 200908, 2020.

[4] Z. Salsabila, P, “Cybercrime in Indonesia Rises 4-fold During the Pandemic,” *Kompas.com*, 2020. https://tekno.kompas.com/read/2020/10/12/07020007/kejahatan-siber-di-indonesia-naik-4-kali-lipat-selama-pandemi.

[5] M. Libicki, “Could the Issue of DPRK Hacking Benefit from Benign Neglect?,” *Georg. J. Int. Aff.*, vol. 19, pp. 83–89, 2019, doi: DOI: https://doi.org/10.1353/gia.2018.0010.

[6] J. Fadhilah, C. A. A. Layyinna, R. Khatami, and F. Fitroh, “Utilization of Digital Wallet Technology as Alternative Solution of Modern Payment: Literature Review,” *J. Comput. Sci. Eng.*, vol. 2, no. 2, pp. 89–97, 2021, doi: 10.36596/jcse.v2i2.219.

[7] P. Roszkowska, “Fintech in financial reporting and audit for fraud prevention and safeguarding equity investments,” *J. Account. Organ. Chang.*, vol. 17, no. 2, pp. 164–196, 2021, doi: 10.1108/JAOC-09-2019-0098.

[8] S. Varga, J. Brynielsson, and U. Franke, “Cyber-threat perception and risk management in the Swedish financial sector,” *Comput. Secur.*, vol. 105, p. 102239, 2021, doi: 10.1016/j.cose.2021.102239.

[9] A. B. Jibril, M. A. Kwarteng, R. K. Botchway, J. Bode, and M. Chovancova, “The impact of online identity theft on customers’ willingness to engage in e-banking transaction in Ghana: A technology threat avoidance theory,” *Cogent Bus. Manag.*, vol. 7, no. 1, 2020, doi: 10.1080/23311975.2020.1832825.

[10] J. Kim, J. Nam, D. Jeon, and B. Administration, “A Study on Reuse Intention of the Easy Payment Service,” *J. Digit. Converg.*, vol. 16, no. 11, pp. 303–312, 2018.

[11] A. Muaz, M. Jayabalan, and V. Thiruchelvam, “A comparison of data sampling techniques for credit card fraud detection,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 6, pp. 477–485, 2020, doi: 10.14569/IJACSA.2020.0110660.

[12] B. Al-Shargabi, S. Al-Jawarneh, and S. M. A. Hayajneh, “A cloudlet based security and trust model for e-government web services,” *J. Theor. Appl. Inf. Technol.*, vol. 98, no. 1, pp. 27–37, 2020.

[13] C. Conradt, “Online auction fraud and criminological theories: The Adrian Ghighina case,” *Int. J. Cyber Criminol.*, vol. 6, no. 1, pp. 912–923, 2012.

[14] PwC, “Fighting fraud: A never-ending battle PwC’s Global Economic Crime and Fraud Survey 2 0 2 0,” p. 14, 2020.

[15] M. Elyas, S. B. Maynard, A. Ahmad, and A. Lonie, “Towards a systemic framework for digital forensic readiness,” *J. Comput. Inf. Syst.*, vol. 54, no. 3, pp. 97–105, 2014, doi: 10.1080/08874417.2014.11645708.

[16] R. Hikmatulloh and E. Nurmiati, “Analisis Strategi Pencegahan Cybercrime Berdasarkan UU ITE Di Indonesia (Studi Kasus: Penipuan Pelanggan Gojek),” *Kosmik Huk.*, vol. 20, no. 2, p. 121, 2020, doi: 10.30595/kosmikhukum.v20i2.6449.

[17] D. Sugianto, “BI Records 3.4 Million Merchants in Jakarta Already Connected to QRIS,” *Finance.Detik.Com*, 2022. .

[18] Sugiyono, *Metode Education Research. Approach Quantitative, Qualitative, and R & D*. Bandung: Alfabeta, 2011.

[19] M. Sarstedt, C. M. Ringle, and J. F. Hair, *Handbook of Market Research*, no. September. Hamburg: Springer International Publishing, 2017.

[20] et al Hair, *A Primer On Partial Least Squares Least Structural Equation Modeling (PLS-SEM)*. SAGE Publications, 2014.

[21] I. Ghozali and L. Hengky, *Concept, Technique and Application to Use Program of Smart PLS 3.0*. 2015.

[22] J. F. Hair, J. J. Risher, and C. M. Ringle, "When to use and how to report the results of PLS-SEM," vol. 31, no. 1, pp. 2–24, 2018, doi: 10.1108/EBR-11-2018-0203.

[23] U. Sekaran and R. Bougie, *Research Methods For Business : A Skill Building Approach*, 7th, abrigat ed. John Wiley & Sons, 2016, 2016.

[24] U. Sekaran and R. Bougie, "Research Methods For Business. A Skill Builing Approch. 7th Edition," *Book*, 2016, doi: 10.1007/978-94-007-0753-5_102084.

[25] M. Riek, R. Böhme, M. Ciere, C. Gañán, and M. Van Eeten, "Estimating the costs of consumer-facing cybercrime: A tailored instrument and representative data for six EU countries," *Work. Econ. Inf. Secur.*, pp. 1–43, 2016.

[26] H. F. Atlam, A. Alenezi, M. O. Alassafi, A. A. Alshdadi, and G. B. Wills, "Security, Cybercrime and Digital Forensics for IoT," *Intell. Syst. Ref. Libr.*, 2019.

[27] Y. Prayudi, A. Ashari, and T. K Priyambodo, "A Proposed Digital Forensics Business Model to Support Cybercrime Investigation in Indonesia," *Int. J. Comput. Netw. Inf. Secur.*, vol. 7, no. 11, pp. 1–8, 2015, doi: 10.5815/ijcnis.2015.11.01.

[28] M. K. Khando, S. Gao, S. Islam, and A. Salman, "Enhancing employees information security awareness in private and public organizations : A systematic literature review," *Comput. Secur.*, vol. 106, 2021.