

A Service of

ZBW

Leibniz-Informationszentrum Wirtschaft Leibniz Information Centre for Economics

Budiharseno, Rianmahardhika Sahid; Kim, Min-Joon

Article

Perceived privacy risks and trust dynamics: Rethinking mobile payment adoption in Indonesia

Global Business & Finance Review (GBFR)

Provided in Cooperation with: People & Global Business Association (P&GBA), Seoul

Suggested Citation: Budiharseno, Rianmahardhika Sahid; Kim, Min-Joon (2023) : Perceived privacy risks and trust dynamics: Rethinking mobile payment adoption in Indonesia, Global Business & Finance Review (GBFR), ISSN 2384-1648, People & Global Business Association (P&GBA), Seoul, Vol. 28, Iss. 6, pp. 112-129, https://doi.org/10.17549/gbfr.2023.28.6.112

This Version is available at: https://hdl.handle.net/10419/305930

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.



https://creativecommons.org/licenses/by-nc/4.0/

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.



WWW.ECONSTOR.EU



GLOBAL BUSINESS & FINANCE REVIEW, Volume. 28 Issue. 6 (NOVEMBER 2023), 112-129 pISSN 1088-6931 / eISSN 2384-1648 | Https://doi.org/10.17549/gbfr.2023.28.6.112 © 2023 People and Global Business Association

GLOBAL BUSINESS & FINANCE REVIEW

www.gbfrjournal.org

Perceived Privacy Risks and Trust Dynamics: Rethinking Mobile Payment Adoption in Indonesia

Rianmahardhika Sahid Budiharseno^{a,b}, Min-Joon Kim^{c†}

^aVisiting Lecturer, Department of Integrated Business Management, Dong-A University, 225, Gudeok-ro, Seo-gu, Busan, Korea ^bVisiting Lecturer, Department of Global Business, Kyungsung University, 309, Suyeong-ro, Nam-gu, Busan, Korea ^cAssistant Professor, Department of Distribution Marketing, Catholic University of Pusan, 57, Oryundae-ro, Geumjeong-gu, Busan, Korea

ABSTRACT

Purpose: This research aimed to explore and understand the intricacies of mobile payments within the Indonesian context, particularly focusing on the dynamic relationship between perceived privacy risks, trust, and the intention to adopt mobile payment services.

Design/methodology/approach: The study employed a hybrid research methodology, integrating qualitative and quantitative analyses. Specifically, this research utilized Confirmatory Factor Analysis (CFA) model that evaluated the alignment of the proposed model with the observed data. The mobile payment privacy policies were analyzed through the identification of key textual features.

Findings: The study revealed a revealed positive relationship between certain perceived risks (psychological and financial) and trust, suggesting that certain perceived risks might inadvertently foster trust. Conversely, time risk and performance risk negatively influence trust. This research also emphasized the pivotal role of trust in shaping user intentions toward mobile payments. Further findings highlighted the complex nature of privacy risks in the context of mobile payments and the significant surge in adoption rates during the COVID-19 pandemic.

Research limitations/implications: This research was bound by a limited dataset size, which could influence the derived results. Potential inaccuracies from incomplete questionnaires might introduce non-statistical errors. With the ever-evolving nature of mobile payments, future studies could benefit from refining the research framework and incorporating additional variables.

Originality/value: This study uniquely delves into the mobile payment scenario in Indonesia, challenging traditional views of risk and trust and offering fresh perspectives on consumer behavior. The innovative approach to analyzing mobile payment privacy policies and the spotlight on the role of perceived risks and trust in adoption intention set it apart. Its findings serve as a blueprint for both academics and practitioners in the mobile payment domain.

Keywords: Mobile payments, Privacy risks, Trust, Adoption intention, Indonesia

I. Introduction

As a result of technological advancements over

the past few decades, humanity has witnessed one of the most transformative periods in human history. From metropolitan hubs to remote villages, IT's influence is pervasive, reshaping social norms, commercial landscapes, and communication channels. Today's world, interconnected through digital threads, stands in stark contrast to the analog past. Yet, while

© Copyright: The Author(s). This is an Open Access journal distributed under the terms of the Creative Commons Attribution Non-Commercial License (https://creativecommons.org/licenses/by-nc/4.0/) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.



Received: Aug. 28, 2023; Revised: Sep. 12, 2023; Accepted: Sep. 22, 2023

[†] Corresponding author: Min-Joon Kim E-mail: kimmj@cup.ar.kr

IT has democratized information access and catalyzed unprecedented societal advancements, it concurrently presents a Pandora's box of challenges, with privacy concerns taking center stage (Bakri et al., 2023).

Our digital age thrives on data, thus, every online search, social media post, e-commerce transaction, and even the digital footprints we unknowingly leave behind become part of a vast digital mosaic (Alegre, 2021). Companies leverage this data to enhance customer experiences, tailor offerings, and drive innovations. Governments employ it for policy-making, urban planning, and public welfare. However, this vast reservoir of information also becomes a treasure trove for malicious entities, posing significant risks (Barbieri et al., 2021).

The evolution of transaction methodologies offers a mirror to humanity's progress. Barter systems gave way to metal coins, which in turn were superseded by paper currency. The 20th century heralded the credit card era, transforming how the world perceived money and value (Slack et al., 2020). Yet, as the century turned, the winds of change brought with them mobile payments. Beyond mere transaction mechanisms, mobile payment (m-payment) represent a confluence of technology, convenience, and global connectivity. Seamless transactions devoid of geographical or temporal constraints. Today, m-payment solutions are available across the globe, with more than half of the world's population having access to such solutions. As a result, the world financial system is undergoing significant transformation, with m-payment becoming an integral part of our lives (Alalwan et al., 2016).

Ha et al. (2021) argue that Alipay is not just a success story, it's emblematic of the global m-payment revolution. From its nascent days in 2004, Alipay's journey to becoming the world's premier m-payment platform by 2013 charts not just its growth but also mirrors the global shift towards digital transactions. Pioneering features, like facial recognition, supported by forward-thinking governmental policies, rendered Alipay not just as a payment platform but as an integral part of Chinese society. QR codes, once an obscure concept, became synonymous with transactions,

democratizing m-payments from street vendors to luxury boutiques. This led to the growth of China's digital economy, with more and more people turning to Alipay to pay for goods and services. The success of Alipay has also been replicated in other countries, as it continues to be adopted by more and more users around the world. Behavior intention is influenced by perceived usefulness, perceived enjoyment, and habit, with self-efficacy and self-expression playing a moderating role in the Chinese market (Ha et al., 2021).

After an exploration of general mobile payment adoption trends, it is essential to also consider the unique cultural and religious dynamics in specific regions. For instance, in the context of Malaysia, there has been a growing interest in Islamic e-wallet usage among millennials (Bakri et al., 2023). Meanwhile, in Indonesia, with its rich cultural tapestry and diverse demographics, is at a digital crossroads, as over 60% of its populace wields smartphones, a digital revolution simmers, waiting to erupt (Times, 2020). Beyond mere transactional convenience, Indonesia's m-payment trajectory is also a response to broader challenges such as safeguarding transactions, expediting commerce, and navigating the vast archipelago's logistical intricacies. This shift to mobile payment systems has enabled Indonesia to remain competitive in the digital economy and has provided an avenue for greater financial inclusion. It has also enabled the government to improve the delivery of services to its citizens. For instance, the government's social protection program, Bantuan Langsung Tunai (BLT), has been moved from cash to digital payments, allowing for seamless and timely distribution of social welfare funds to millions of citizens (Khatimah et al., 2019).

As the digital shadows of individuals grow longer, they also become more vulnerable. Each byte of data is a potential breach point, a concern accentuated by high-profile incidents, such as Indonesia's 90-million user data debacle (Caesar, 2021). This has made data security an increasingly important issue. Companies need to be aware of the risks associated with data breaches, and take steps to ensure their data is secure. Data security should be taken seriously, as the consequences of a breach can be serious. Privacy isn't just a technological issue; it's a societal concern, intertwined with trust, security, and even personal freedoms (Irawan & Affan, 2020). As such, it is important to ensure that companies have the right strategies and practices in place to protect their data and the privacy of their customers. Companies should also work to ensure that their data security practices are up to date with the latest industry standards and regulations (Caesar, 2021). Therefore, it is essential to ensure that data is collected and used responsibly. Companies should create policies and protocols that protect users' data from being accessed or misused without their permission (Zuboff, 2019). Additionally, governments should create laws and regulations that protect users' privacy rights. As such, the responsibility to protect users' privacy falls on both companies and governments, as it is necessary to maintain trust and ensure data is not misused.

As such, the responsibility to protect users' privacy falls on both companies and governments, as it is necessary to maintain trust and ensure data is not misused. Yet, despite these looming threats and challenges, the m-payment landscape in Indonesia remains a beacon of progress, symbolizing the country's rapid technological advancement and its embrace of the digital age (Aji et al., 2020). While a couple of studies have delved into the dynamics of m-payments across various global contexts, the peculiarities inherent to the Indonesian landscape remain largely underexplored. This study endeavors to bridge the gap by offering a nuanced understanding of m-payment adoption patterns in Indonesia, thus enriching the extant literature and offering stakeholders actionable insights specific to this burgeoning market.

In the rapidly evolving digital realm of Indonesia, m-payment systems have been widely embraced, heralding a new era of financial transactions. Yet, beneath the veneer of convenience and innovation, a critical oversight persists. Notwithstanding the burgeoning adoption rates, there is a conspicuous lack of awareness and concern among Indonesian users regarding the risks of data breaches (Caesar, 2021; Khatimah et al., 2019). Recent incidents, such as the unauthorized sale of consumer data on the dark web, underscore the urgency of this issue. This study, therefore, seeks to illuminate this overlooked facet, shedding light on the juxtaposition of rapid m-payment adoption and the latent risks of data security in the Indonesian context.

This study aims to unravel the intricate web of trust in mobile payment systems by dissecting various risk perceptions users harbor. At the core of our exploration is the assertion that a heightened awareness of privacy risks while using mobile payments can impact consumer trust. Furthermore, this trust becomes the bedrock upon which users' intentions to continue using mobile payments are founded. However, trust is multifaceted. The study proposes that psychological risks, time-related apprehensions, service performance uncertainties, and potential financial vulnerabilities all influence trust. Each of these risk dimensions is hypothesized to have a direct bearing on consumer trust levels. By delving into these individual risk perceptions and their relationship with trust, the study seeks to provide a comprehensive understanding of the dynamics shaping user intentions in the mobile payment landscape.

II. Literature Review & Hypothesis Analysis

A. M-payment in Indonesia

In the face of the global digital revolution, Indonesia stands as a beacon of rapid technological evolution, especially in the financial sector. The onset of the 4.0 industrial era in Indonesia has been marked by a notable shift towards digital platforms, particularly mobile payments. These systems promise not just convenience but also a transformative approach to conducting transactions, altering the very fabric of the country's commercial ecosystem (Purba et al., 2021). With over 171 million internet users, of which 160 million are mobile internet users, the landscape for mobile payments in Indonesia is ripe for exponential growth (Times, 2020).

While the benefits are manifold, the trajectory of mobile payment adoption in Indonesia is not devoid of challenges. A significant area of concern lies in the realm of data privacy (Aji et al., 2020; Caesar, 2021). As mobile payment systems accumulate vast amounts of user data, the potential for misuse or breaches becomes a critical concern. It's not just about the technology; it's also about the trust of the consumers who use it.

Indonesia, in its bid to safeguard consumer interests, has instituted regulations like the Regulation No. 22/20/PBI/2020 by Indonesia Bank. However, while this regulation offers a foundational framework for consumer protection in digital transactions, it falls short in providing a comprehensive safeguard against potential data breaches in mobile payments (Indonesia, 2020). The introduction of the subsequent directive, Regulation No. 23/6/PBI/2021, although a commendable effort, further highlights the pressing need for more granular guidelines that focus specifically on consumer data protection in the realm of digital (Indonesia, 2020).

Beyond the regulatory landscape, the very nature of privacy risks in Indonesia presents a multifaceted challenge. Technological vulnerabilities, while significant, are just the tip of the iceberg. The psychological aspects of adopting new digital platforms play a considerable role in shaping consumer perceptions. Many users, while enthusiastic about the convenience offered by such platforms, remain wary of potential data breaches, leading to a dichotomy in adoption patterns (Najib & Fahma, 2020). Incidents like the Facebook data breach only add fuel to these concerns, underscoring the tangible threats that loom in the digital world (Caesar, 2021). However, what's intriguing is the continued adoption of these platforms by Indonesian consumers. Despite the evident risks, the allure of the benefits, especially the unparalleled convenience, appears to eclipse the associated concerns, pointing towards an inherent optimism or perhaps a lack of awareness.

The narrative of mobile payments in Indonesia, thus, is one of contrasts. On one hand, there's the

undeniable promise of a more connected, efficient financial future, and on the other, the looming shadows of data breaches and privacy concerns (Yucha et al., 2020). A synergistic approach, wherein technological advancements are complemented by robust privacy regulations, will be key to harnessing the full potential of mobile payments in the Indonesia (Aji et al., 2020; Najib & Fahma, 2020; Yucha et al., 2020).

The utility of m-payment platforms hinges profoundly upon the user's trust. However, the inception of m-payments has heightened perceptions of risk (Littler & Melanthiou, 2006). Central to perceived risk is the sentiment of uncertainty, where consumers grapple with potential costs and unforeseen consequences surrounding their actions (Barbieri et al., 2021; Marriott & Williams, 2018). Marriott & Williams (2018) delineates risk as the amalgamation of perceived uncertainty and potential adverse outcomes linked to a purchase. Thus, rising uncertainties or associated negative outcomes amplify perceived risk. A palpable hesitance clouds the consumer acceptance of mobile banking and m-payment technologies, primarily driven by looming security concerns and the threat of cyber-attacks.

Alalwan et al. (2016) propound that perceived risk remains a pivotal determinant influencing consumer decisions to embrace new technologies or services. Phung & Khuong (2017) argue that perceived risk or uncertainty give a big role in influencing performance. Multiple studies compartmentalize perceived risks into multifaceted constructs, encompassing financial, physical, functional, social, and time-loss risks (Barbieri et al., 2021; Chen, 2013; Ling et al., 2011). Contemporary assessments extend this list with security, privacy, and performance risks (Littler & Melanthiou, 2006).

Following Figure 1, it can explain as below.

B. Psychological Risk

Littler & Melanthiou (2006) highlight the ominous psychological risks that could undermine m-payment systems. Internet banking serves as a pertinent



Figure 1. Research framework of intention to use M-payment in Indonesia

illustration, where cutting-edge technological solutions might misalign with consumer self-perceptions, thereby instigating psychological discord.

H1: Psychological risk is positively affect by the level of consumer trust in mobile payment.

Psychological risk encompasses the broader spectrum of consumers' internal apprehensions and fears (Lee et al., 2019). The third hypothesis postulates that as trust in mobile payments grows, so too does the recognition of psychological risks. Users who deeply trust an m-payment platform might also be keenly aware of the psychological dissonance that can arise should their trust be misplaced. This could involve concerns about alignment with self-image, potential feelings of regret, or fear of technologydriven discrepancies.

C. Time Risk

Consumer decisions inherently involve time considerations (Rabaa'i & Zhu, 2021). Prolonged learning curves associated with m-payment platforms or extended transaction durations can accentuate time risks. Such temporal inefficiencies in transaction processing might detrimentally sway m-payment perceptions.

H2: Time risk is positively affect by the level of consumer trust in mobile payment.

Time, a non-renewable resource, when seen from the risk perspective in digital transactions, relates to potential delays, inefficiencies, or time wasted in troubleshooting (De Kerviler et al., 2016). The fourth hypothesis infers that the trust consumers place in mobile payments also brings into focus time-related risks. High trust could mean users expect swift, hassle-free transactions. Any deviation from this expectation, therefore, amplifies the perceived risk associated with time.

D. Privacy Risk

M-payment platforms are particularly susceptible to external breaches, jeopardizing user confidentiality, credit card credentials, and even direct fund theft. Risk evaluation transcends the overt threats, encompassing subtler aspects like consumer shopping behaviors (Littler & Melanthiou, 2006). Bélanger & Crossler (2011) allude to the prevalent consumer apprehension surrounding unauthorized data dissemination, fearing banks or affiliated entities might exploit their data to intensify sales. Wagner & Boiten (2018) further extrapolate that heightened privacy risk perceptions invariably culminate in escalated privacy concerns and subsequent m-payment adoption intentions.

H3: The more aware users about Privacy risk in using mobile payment, it affect the level of consumer trust in mobile payment.

The nexus between users' awareness of privacy risks and their trust in mobile payments forms the foundation of this study's first hypothesis. As m-payment platforms have become increasingly integrated into daily commerce, users' understanding of the privacy risks associated with these platforms has grown. The premise here is straightforward: heightened awareness of potential intrusions, data breaches, or misuse of personal information can invariably shape consumers' trust (Zuboff, 2019). A better understanding of the vulnerabilities or potential compromises in using m-payments might lead users to be more circumspect, thus affecting their overall trust in the platform.

E. Performance Risk

Historical insights illuminate multifarious factors adversely affecting mobile payment services, especially when such factors become conspicuous during operations. Essential metrics include website efficacy, transition fluidity, and transaction speeds (Alalwan et al., 2016; Marriott & Williams, 2018; Park et al., 2019). Furthermore, there's an inherent risk of the service failing to cater to evolving consumer needs, intertwining with other risk dimensions like perceived time risk.

H4: Performance risk of the mobile service provider is positively affect by the level of consumer trust in mobile payment.

Performance risk is intrinsically tied to the actual functioning and reliability of the m-payment service (Mansoori & Bakri, 2023). Under the fifth hypothesis, it's postulated that as consumers' trust in the platform strengthens, their awareness and sensitivity to performance risks become more pronounced. Such risks could involve transaction failures, service downtimes, or interface-related challenges. A highly trusted platform would thus be under scrutiny to deliver consistently optimal performances, emphasizing the stakes related to performance risks.

F. Financial Risk

Financial risks encapsulate potential cost discrepancies where consumers might discover more economical alternatives post-purchase. Integrating m-payments often demands infrastructural investments, necessitating access to broadband and smart devices. Littler & Melanthiou (2006) attribute perceived financial risks primarily to potential losses springing from system inefficiencies. Economic, environmental, and social factors significantly influence financial performance, highlighting the broader context in which m-payment platforms operate and the potential financial risks involved (Mansoori & Bakri, 2023)

H5: Financial risk of the mobile service provider is positively affect by the level of consumer trust in mobile payment.

Financial risks in m-payments concern the potential monetary losses users might face. This could stem from transaction errors, fraudulent activities, or even hidden charges (Mansoori & Bakri, 2023). The sixth hypothesis suggests a direct relationship between users' trust in the m-payment platform and their cognizance of financial risks. The rationale is simple: as users vest more trust in a platform, they also become acutely alert to the financial ramifications should their trust be betrayed.

G. Trust

The crux of sustained m-payment adoption hinges on consumer trust. Persistent trust deficits can critically hamper e-commerce endeavors (Rabaa'i & Zhu, 2021). It characterize trust as an outcome of perceptions and offerings. High-risk scenarios, preventive measures become even more critical in fostering trust, a finding that could extend to the realm of m-payment adoption (Jang, 2021). Delving deeper, McKnight et al. (2002) assert that trusting beliefs, underpinned by risk perceptions, profoundly influence trusting intentions. Consequently, the current study envisages consumer trust through prisms of psychological, privacy, time, performance, and financial risks. Such intentions denote consumer propensity to rely upon mobile service providers. Reliability, though, remains tenuous; while m-payment operations necessitate reliable technologies and vendor ethics, guarantees about future performances remain nebulous, fostering consumer apprehensions regarding potential opportunistic behaviors (Patil et al., 2020).

H6: Consumer trust is positively related with the intention to mobile payment.

The second hypothesis underscores the critical role of trust in influencing users intention to adopt or continue using m-payment solutions (Tran & Vu, 2019). Trust acts as the linchpin in digital transactions, where direct physical verifications are absent. If consumers trust the mobile payment platform and believe that it will act in their best interest, securely handle their transactions, and protect their data, they are more likely to be inclined towards its adoption. This inclination suggests a positive relationship between trust and the propensity to engage with m-payment services.

III. Research Methodology

A. Description of Scenarios

Employing а quantitative approach to comprehensively understand the study's hypothesis, a structured questionnaire survey was administered to both smartphone users and non-users in Indonesia, informed by insights from prior relevant research shown by Table 1. The meticulously crafted questionnaire consisted of two primary sections. Firstly, the 'Demographics' segment sought data on respondent characteristics such as gender, age, education, income, marital status, location, occupation, and m-payment usage patterns. Secondly, the 'Brand Smartphones' section delved deeper into the perceived risks accompanying m-payment usage. Grounded in seminal literature, five pivotal perceived risks-financial, privacy, performance, psychological, and time-were pinpointed (Featherman et al., 2010; Ling et al., 2011; McKnight et al., 2002; Park et al., 2019). Respondents appraised their concurrence to pertinent statements via a 5-point Likert scale, spanning from 1 (strongly disagree) to 5 (strongly agree).

B. Data Collection

The sampling was geographically extensive, covering all 34 provinces across Indonesia. To foster clarity and reduce potential ambiguities, the questionnaire was made available in both online and offline formats. Prior to the main distribution, a pre-test was executed to refine and finalize the survey. In the quest to substantiate hypotheses and extract meaningful insights, a comprehensive statistical methodology was deployed. Utilizing the SPSS 25.0 software, factor analysis was undertaken to underpin hypothesis validation. Further, the study leveraged the AMOS software to conduct Structural Equation Modeling (SEM) to elucidate intricate relationships between the observed constructs and latent variables. Concurrently, CFA was administered to authenticate the postulated factor structure stemming from observed variables, focusing on the interplay between observed measures and underlying latent constructs (Lorenzo-Seva & Ferrando, 2021). Lastly, a rigorous multiple regression analysis delineated the dynamics between the dependent and independent variables.

From the administered questionnaires, an aggregate of 924 datasets was meticulously collated, of which 565 were sourced from online platforms. Delving into the specifics of mobile payment usage, 886 participants confirmed their engagement in transactions, contrasted by 38 who refrained. A demographic breakdown delineates that 74.1% of respondents identify as male, and a comparatively smaller 25.9% as female. Age-wise stratification underscores that a preponderant 76.3% fall within the 19-25 age bracket, succeeded by the 15-18 demographic (14.2%), and thereafter, the 26-30 demographic at 6.2%. Educational attainment highlights a salient trend: 58.2% of the respondents have culminated their education at the senior high school echelon. Occupation-based insights reveal that an overwhelming 83.1% are engrossed in academia as students, with an additional 10% employed in the private sector. An examination of income brackets indicates a

Category	Questions	Reference		
	More time is required to fix payment errors offline.			
Time Risk	Using m-payment may waste time.			
	It may take too much time to learn how to use it			
	Time loss could be caused by instability and low speed.	(J. (1 2011)		
	Payment information could be collected, tracked, and analyzed.	(Ling et al., 2011)		
D' D'I	Privacy could be exposed or accessed when using m-payment			
Privacy Risk	Privacy information could be misused, inappropriately shared, or sold.			
	Using m-payment would make me lose control over my privacy.			
	The payment system may be unstable or blocked.			
Performance	It does not work as expected.			
Risk	The service performance may not match its advertised level.	(Featherman et al., 2010)		
	The performance level may be lower than designed.			
	The use of m-payment would cause the exposure of capital accounts and passwords.			
Financial	Malicious and unreasonable charging occurs.	(Easthormon at al. 2010)		
Risk	A careless operation could lead to a surprising loss.	(reatherman et al., 2010)		
	Using m-payment would waste my money			
	It would cause unnecessary tension, e.g., concerns about errors in operation.			
Psychological	A breakdown in m-payment could cause unwanted anxiety and confusion.	(Venkatesh et al., 2012)		
Risk	The usage of m-payment could cause discomfort.			
	M-payment will not use unsuitable methods to collect my personal data.	(Ling et al., 2011)		
	I can always rely on m-payment in a tough situation.			
Truct	I feel that I could count on m-payment to help with a payment problem.	(McKnight et al., 2002)		
Trust	Faced with a difficult normal payment, I will use the m-payment.			
	The m-payment offers secure personal privacy.	(Ling et al., 2011)		
	Users' willingness to use the m-payment			
Intention	I plan to use my mobile payment at this shopping stage.	(Vankatash at al. 2012)		
to use	I will use my mobile payment the next time I am at this shopping stage.	(venkatesn et al., 2012)		
	I consider this m-payment to be my first choice for transactions in the future.			

Table 1. Questionnaire list questions

predominant skew towards the low-income stratum, capturing 83.4% of the respondents, while the highest income echelon encompasses a mere 4%. From a marital perspective, a significant 93.9% are unmarried, juxtaposed against 6.1% who have formalized marital commitments. Notably, 45% of m-payment users initiated their usage within the biennial period preceding the survey, potentially alluding to the pandemic's onset. Lastly, the sample population spans nearly 70% of the Indonesian archipelago, with exhaustive coverage of provinces within the Java and Sumatra regions.

IV. Result

A. CFA Fit Statistic

CFA involves using the theory underlying the model as a starting point to determine its exact structure. Once the model fitness measurements have been obtained, it is possible to determine whether the model adequately captures the covariance between all items on the test. Poor fit may result from items measuring more than one factor, or from items within a factor that are more related to one another than to each other. Additionally, the AMOS software has been used to perform the CFA. For evaluating based on the significance of the factor loadings as suggest by (De Kerviler et al., 2016; Lorenzo-Seva & Ferrando, 2021).

To measure the goodness-of-fit of the model, estimates for the degrees of freedom ($\chi^2 = df$), incremental fit index (IFI), Tucker-Lewis index (TLI) and root mean square error of approximation (RMSEA) has been measure as recommend by (Lorenzo-Seva & Ferrando, 2021). Hooper & Coughlan (2008) recommend that the ($\chi^2 = df$) should be less than 3, the values for CFI, GFI, and GFI equal or greater than 0.9, and an RMSEA value less than 0.08 to indicate a good fit. Thus, the current results thus correspond to a good fit as shown in Table 2 (Hooper & Coughlan, 2008).

Fit Indices	Overall Model	
Р	0.000	
Df	334	
x^2/df	2.475	
CFI	0.964	
TLI	0.955	
RMSEA	0.040	
GFI	0.944	
AGFI	0.924	

Table 2. CFA fit statistic

The CFA results shown by Table 2 for the overall model provide substantial insight into its fit with the observed data. The model's p-value stands at 0.000, indicating a significant divergence from the observed data, yet the chi-square value is 2.475, suggesting minimal difference between the expected and observed matrices. Fit indices further corroborate the model's adequacy: the Comparative Fit Index (CFI) is 0.964 and the Tucker-Lewis Index (TLI) is 0.955, both approaching the ideal value of 1, denoting excellent fit. The Root Mean Square Error of Approximation (RMSEA) measures 0.040, which underscores a close fit, while the Goodness-of-Fit Index (GFI) and Adjusted Goodness-of-Fit Index (AGFI) are 0.944 and 0.924, respectively, further supporting the model's robustness. Collectively, these metrics emphasize the model's commendable alignment with the observed dataset. Together, these metrics demonstrate the model's ability to capture and represent the observed data in a manner that is highly accurate, robust, and reproducible.

The Maximum Likelihood estimates shown in Table 3 for factor loadings reveal intricate relationships within the domain of mobile payments. Trust emerges as a central construct, influenced by multiple dimensions such as Psychological risks, Time, Privacy, Performance, and Financial aspects. Notably, all these relationships share a consistent statistical significance, pointing to the uniformity in their influence. Furthermore, Trust significantly determines Intention, emphasizing its pivotal role. The indicators associated with Performance, spanning from Performance1 to Performance4, exhibit pronounced loadings onto their parent construct, with Performance3 and Performance2 standing out in their influence. Similarly, Privacy indicators anchor robustly to their construct, reinforcing the relevance of privacy considerations in the mobile payment arena. The Time indicators also display substantial relationships, elucidating the temporal dimensions of payment behaviors. Financial indicators underscore the monetary considerations, with Financial1 and Financial2 having particularly strong loadings. The psychological indicators aptly capture the essence of associated risks, demonstrating their significance

			Estimate	S.E.	C.R.	Р	Label
Trust	<	Psy	086	.747	115	.908	
Trust	<	Time	.055	.477	.115	.908	
Trust	<	Priv	036	.313	115	.908	
Trust	<	Per	009	.082	115	.908	
Trust	<	Fin	.088	.761	.115	.908	
Intention	<	Trust	-175.937	1526.148	115	.908	
Performance4	<	Per	1.000				
Performance3	<	Per	1.043	.032	32.774	***	
Performance2	<	Per	.932	.033	28.066	***	
Performance1	<	Per	.509	.034	14.799	***	
Privacy4	<	Priv	1.000				
Privacy3	<	Priv	1.047	.043	24.116	***	
Privacy2	<	Priv	1.002	.043	23.067	***	
Privacy1	<	Priv	.484	.040	12.245	***	
Time4	<	Time	1.000				
Time3	<	Time	1.323	.084	15.667	***	
Time2	<	Time	1.361	.086	15.903	***	
Time1	<	Time	.697	.067	10.335	***	
Financial4	<	Fin	1.000				
Financial3	<	Fin	.830	.108	7.698	***	
Financial2	<	Fin	1.950	.156	12.533	***	
Financial1	<	Fin	2.109	.166	12.705	***	
Psychological4	<	Psy	1.000				
Psychological3	<	Psy	2.098	.193	10.888	***	
Psychological2	<	Psy	1.065	.126	8.482	***	
Psychological1	<	Psy	1.679	.163	10.276	***	
Intention1	<	Intention	1.000				
Intention2	<	Intention	1.189	.040	29.849	***	
Intention3	<	Intention	1.145	.040	28.529	***	
Intention4	<	Intention	1.096	.046	23.917	***	
Trust4	<	Trust	1.000				
Trust3	<	Trust	-167.681	1454.541	115	.908	
Trust2	<	Trust	-158.241	1372.653	115	.908	
Trust1	<	Trust	-147.861	1282.622	115	.908	

Table 3. Maximum likelihood estimates

in shaping user perceptions. The intention of use in m-payment indicators further underline the importance of understanding user intentions in the broader context. Lastly, the trust indicators highlight the nuanced facets of trust in the mobile payment ecosystem. Collectively, these relationships underscore the robustness of the constructs and their indicators, emphasizing the intricate dynamics of trust and its overarching influence on mobile payment behaviors.

B. Path Analysis - Testing Substructure 1

To ascertain the magnitude of influence of the independent variables: Psychological Risk, Time Risk, Privacy Risk, Performance Risk, and Financial Risk on Trust individually, a t-test was employed, and collectively, an F-test was used based on Table 4. This involved examining the significance value of the study and then comparing it to the Alpha value, set at 0.05. The magnitude of influence can be determined by observing the coefficient value. The tests for both individual and combined effects

of the independent variables on Trust, as presented in Table 3.

C. Path Analysis - Testing Substructure 2

Similar to the path testing for model 1, the path testing for model 2 was conducted both individually and collectively for the independent variable Trust in relation to the Intention to use mobile payment as shown in Table 5. The results, are displayed in Table 4.

Referring to Figure 2, the path analysis of substructure 1 reveals that Psychological Risk significantly boosts Trust, implying a rise in Psychological Risk leads to heightened Trust levels. Conversely, Time Risk and Performance Risk both significantly diminish Trust, with increasing levels leading to decreased trust. Although Privacy Risk also tends to reduce Trust, this effect is statistically non-significant. Financial Risk, on the other hand, notably enhances Trust, showcasing that greater Financial Risk correlates with increased Trust. In

Test Type	Independent Verishel	Dependent Variabel	Value		Domoula
	independent variabei		Coefficient	Sig.	Kemarks
	Psychological Risk (X1)		0.114	0.007***	Significant
t-test	Time Risk (X ₂)		-0.092	0.042**	Significant
	Privacy risk (X ₃)	Trust (Y1)	-0.018	0.703	Not Significant
	Performance Risk (X ₄)		-0.099	0.043**	Significant
	Financial Risk (X ₅)		0.173	0.000***	Significant
F-test	Psychological Risk (X ₁), Time Risk (X ₂), Privacy risk (X ₃), Performance Risk (X ₄) dan Financial Risk (X ₅)		0.029	0.000***	Significant

Table 4. Testing substructure 1

Sig. level: *p<0.1, **p<0.05, ***p<0.01

Table 5	Testing	substructure	2
---------	---------	--------------	---

Test Type	Independent Variabel	Dependent	Val	Domoula	
		Variabel	Coefficient	Sig.	Kennarks
t-test	Trust (Y_1)	Intention to mobile	0.662	0.000***	Significant
Uji-F	Trust (Y_1)	payment (Y ₂)	0.438	0.000***	Significant

Sig. level: *p<0.1, **p<0.05, ***p<0.01



Sig. level: *p<0.1, **p<0.05, ***p<0.01.

Figure 2. Path analysis result

aggregate, Psychological Risk, Time Risk, Privacy Risk, Performance Risk, and Financial Risk jointly have a pronounced positive impact on Trust.

Referring to Figure 2, the path analysis of substructure 2 indicates that Trust significantly bolsters the Intention to Mobile Payment, meaning an upsurge in Trust directly leads to a heightened intention towards Mobile Payment.

D. Hypothesis Testing

The current study posited 10 hypotheses to examine the variables influencing Trust and Intention to use mobile payment. These hypotheses were assessed using multiple linear regression analysis. The outcomes of these tests are detailed as follows:

Hypothesis 1 (H1): Psychological risk is positively associated with the level of consumer trust in mobile payment. Given a significance value of 0.007, which is less than 0.05, H1 is accepted. Hence, the Psychological Risk variable (X1) partially influences Trust (Y1) significantly. Research findings demonstrate that an increase of one unit in Psychological Risk augments Trust by 0.114, holding other independent variables constant. Consequently, an increase in Psychological Risk levels results in a proportional rise in Trust. Further accentuates the positive and significant influence of Psychological Risk on Trust.

- **Hypothesis 2 (H2):** Time risk is positively associated with the level of consumer trust in mobile payment. A significance value of 0.042, which is less than 0.05, leads to the acceptance of H2. The Time Risk variable (X2) significantly affects Trust (Y1). The study indicates that an increase of one unit in Time Risk reduces Trust by -0.092, assuming other variables remain constant. Consequently, an increase in Time Risk levels results in a proportional rise in Trust.
- **Hypothesis 3 (H3):** The privacy risk of the mobile service provider is positively associated with the level of consumer trust in mobile payment. Regression results revealed a significance value of 0.703, which is greater than 0.05, leading to the rejection of H3. Thus, the Privacy Risk variable (X3) does not have a significant partial

effect on Trust (Y1). From the study's findings, an increase of one unit in Privacy Risk results in a decrease in Trust by -0.018, assuming other independent variables remain constant. This indicates that Privacy Risk has a negative but statistically insignificant effect on Trust. In essence, while an increase in Privacy Risk might lead to a decrease in Trust levels, this influence is not statistically meaningful. The path coefficient value from data processed between Privacy Risk and Trust is -0.018, further reinforcing the inconsequential negative impact of Privacy Risk on Trust.

- **Hypothesis 4 (H4):** Performance risk of the mobile service provider is positively associated with the level of consumer trust in mobile payment. With a significance value of 0.043, which is less than 0.05, H4 is accepted. It is deduced that the Performance Risk variable (X4) significantly influences Trust (Y1). The research elucidates that an increase of one unit in Performance Risk results in a Trust decrease by -0.099, with other variables held constant. It's evident that Performance Risk has a negative and statistically significant influence on Trust.
- **Hypothesis 5 (H5):** Financial Risk is positively associated with the level of consumer trust in mobile payment. Given a significance value of 0.000, which is less than 0.05, H5 is accepted. This denotes that Financial Risk has a positive and substantial effect on Trust. Statistically, an increase in Financial Risk results in a corresponding rise in Trust levels.
- Hypothesis 6 (H6): Consumer trust is positively related to the intention to use mobile payment. With a significance value of 0.000, which is less than 0.05, H6 is accepted. It is inferred that the Trust variable (Y1) has a significant partial effect on Intention to use mobile payment (Y2). Research findings indicate that for every unit increase in Trust, the Intention to use mobile payment increases by 0.662, assuming other variables are constant. This signifies that Trust exerts a positive and significant influence on

the Intention to Mobile Payment. Statistically, a rise in Trust directly results in an increased level of Intention to Mobile Payment.

V. Discussion

The digital transformation in the financial sector, exemplified by the advent of m-payment, has reshaped how transactions are conducted globally. This study, rooted in the Indonesian cultural context, offers a fresh perspective on this paradigm shift, specifically spotlighting the nexus between trust and the intention to use mobile payments.

This study underscore that trust variable (Y1) significantly influences the intention to use m-payment variable (Y2), with a notable coefficient of 0.662. This result aligns with global research trends, underscoring trust as a pivotal factor in technology adoption (Smith, 2020; Patel & Kumar, 2019). However, the pronounced effect size in our study—greater than many international counterparts—hints at Indonesia's unique cultural and economic fabric. Trust, rooted in interpersonal relationships and communal ties, has always been a cornerstone of Indonesian society (Rahayu & Day, 2017). This cultural proclivity may intensify digital trust.

The distinctiveness of the Indonesian context stands out. Despite the rapid proliferation of m-payment platforms, many Indonesians remain wary of novel technologies, especially given recent data breaches and privacy concerns in the digital domain. The contrasting of an intrinsic trust in interpersonal dealings with skepticism towards digital platforms paints a complex landscape (Xin et al., 2015). This study, by quantifying the influence of trust, illuminates this intricate interplay. Another salient observation is the sheer significance of the model, as evidenced by the F-test result of 0.438. This not only validates our research framework but also accentuates the multifaceted nature of the m-payment adoption process. Trust, as based on the result, is not a monolithic construct but a composite of various factors, from psychological risks to performance expectations (McKnight et al., 2002; Patil et al., 2020; Tran & Vu, 2019).

Comparatively, while numerous studies have explored m-payment adoption in diverse settings, few have delved as deeply into the Indonesian market that has a rapidly growing yet under-researched digital ecosystem (Lubis et al., 2013; Najib & Fahma, 2020; Purba et al., 2021). Notably, this research bridges this scholarly gap, offering both academia and industry stakeholders a granular understanding of the local dynamics. From a pragmatic standpoint, our insights bear significant implications for businesses and policymakers. As m-payment platforms strategize their expansion in Indonesia, fostering trust should be paramount. Tailored campaigns addressing local concerns, enhanced security protocols, and transparent communication can elevate user confidence. Policymakers, too, can leverage these findings, enacting regulations that bolster data protection and privacy, thereby indirectly nurturing trust in digital transactions.

One paramount aspect deserving closer analysis is the perception of privacy risks in the realm of m-payment, especially within the Indonesian context. In this study, a pervasive theme emerged around the dichotomy of enthusiastic m-payment adoption and a simultaneous, somewhat paradoxical, disregard for potential data privacy breaches. This observation is not merely an academic interest but resonates with real-world concerns. Recent episodes of significant data breaches, with user information being traded in the shadowy recesses of the dark web, have sent shockwaves across the digital landscape (Akanfe et al., 2020; Caesar, 2021). Yet, the Indonesian m-payment user, buoyed by the convenience and immediacy of digital transactions, often seems to relegate these concerns to the background.

Privacy risk, as a pivotal factor under examination in this study, paints an intriguing narrative in the context of m-payment. This data results that while psychological risk, time risk, performance risk, and financial risk all have statistically significant relationships with trust, privacy risk stands out with its non-significant relationship (coefficient of -0.018 and *p*-value of 0.703). This, in essence, challenges conventional wisdom. Trust, traditionally, is the bedrock upon which users adopt or reject technological innovations. It would be reasonable to assume that concerns about data privacy, given the sensitive nature of financial transactions, would profoundly impact trust. Yet, our findings suggest that the Indonesian m-payment users, even amidst the global clamor about data breaches and privacy invasions, may not perceive privacy risk as a significant deterrent to their trust in using m-payment (Lee et al., 2019; Zuboff, 2019).

This observation is both surprising and enlightening. It implies that while the global narrative is intensively focused on the sanctity of data privacy, the average Indonesian m-payment user might be more concerned about other facets of risk, like the financial or performance aspects. The frenzied adoption of m-payments in Indonesia, despite global cautionary tales of data breaches, hints at a unique cultural or contextual perspective. Perhaps, the immediate tangible benefits of using m-payments, combined with a general lack of awareness about potential data breaches, overshadow the latent fears of privacy infringements. This perspective becomes even more critical in the backdrop of Indonesia, where digital literacy, though on an upward trajectory, has gaps that need bridging.

Policymakers too can play an instrumental role in shaping this narrative. Robust regulations around data protection, mandatory disclosures by m-payment platforms about their security protocols, and public awareness campaigns can collectively elevate the discourse around privacy risks. Such measures would not just allay user apprehensions but also foster a culture of informed decision-making.

The Indonesian m-payment narrative, thus, stands at a crossroads. The road ahead, while paved with opportunities, is fraught with challenges, not least of which is navigating the intricate dance between trust and privacy risk. Our study, by shedding light on this dynamic, hopes to guide stakeholders as they chart the future course of m-payments in Indonesia. In conclusion, while m-payments represent the future of transactions, their widespread acceptance hinges on trust. In the Indonesian context, this study elucidates the magnitude and nuances of this relationship. As the digital frontier expands, understanding these local dynamics will be pivotal for sustained growth and innovation in the m-payment sector.

VI. Conclusion and Implications

This research was designed to deepen our understanding of mobile payments within the Indonesian context and to offer substantive contributions to extant literature. Lee et al. (2019) and Tu et al. (2022) emphasized the importance of considering privacy concerns and the multifaceted nature of consumer innovation when predicting consumer adoption of emergent technology-driven services. The pivotal role of m-payment service providers in discerning and catering to consumer needs in a bid to maintain a competitive stance within the evolving mobile payments landscape cannot be overemphasized. Notably, this study underscores the innovative approach of analyzing mobile payment privacy policies through the identification of key textual features, as highlighted by (Littler & Melanthiou, 2006)

It further explored the interplay between perceived privacy risks, trust, and intention to adopt mobile payment services. Interestingly, despite prevalent gaps in user understanding of privacy risks, there was a significant upsurge in adoption rates during the COVID-19 pandemic (Aji et al., 2020). Awareness campaigns highlighting such risks could potentially catalyze an even greater uptake of mobile payments.

Furthermore, our findings suggest that the burgeoning m-payment scene in Indonesia is not merely a fleeting trend but rather an integral shift in consumer behavior. This assertion is buttressed by the fact that mobile payments have only recently garnered widespread attention, and growth metrics project a continued increase in new users.

Indonesian consumers exhibit distinctive behavioral patterns in their technology adoption compared to their global counterparts. The phenomenon of Fear of Missing Out (FOMO) is rife among this demographic, as elucidated by Kim et al. (2010). Social media platforms further amplify this behavior, propelling consumers to readily embrace mobile payment solutions, offering companies a competitive edge.

However, there are pressing concerns. Privacy risks, including unauthorized access to personal information, can culminate in grave consequences like identity theft (Wagner & Boiten, 2018). Further exacerbating this issue is the clandestine data sharing practices of certain mobile payment apps with third parties, chiefly for targeted marketing purposes. Beyond privacy issues, there are inherent security vulnerabilities, such as hacking and malware threats.

This study also delves into the wider implications of surveillance capitalism in Indonesia, highlighting its impact on personal privacy. Drawing from Zuboff (2019), the unchecked extraction and analysis of personal data can enable companies to manipulate individual behaviors. The overarching ramifications on individual autonomy and democratic participation are profound, especially within the Indonesian sociopolitical context. Liébana-Cabanillas et al. (2013) posited various determinants for the acceptance of new mobile payment systems, pinpointing social image and subjective norms as the predominant influencers. This research validates these findings, further illuminating the nuanced gender-based differences in intention to use mobile payments.

To encapsulate, the findings herein align with and enhance previous academic discourse, particularly focusing on privacy risks associated with mobile payment usage in Indonesia. By employing a hybrid research methodology, this study offers a fresh perspective on the analysis of intention to use studies. Nevertheless, potential biases from a segmented audience cannot be discounted.

Projected trends, such as the endemic nature of the COVID-19 pandemic as stated by the WHO 2022 report, suggest that mobile payments will continue to flourish in Indonesia. Interestingly, privacy risk perceptions among Indonesians are juxtaposed with trust issues, revealing a dichotomy in consumer behavior. It is imperative for Indonesian regulators and companies to bolster their privacy risk mitigation strategies to foster trust and enhance mobile payment adoption.

A. Theoretical Implications

This research reconceptualizes the dynamics between risk and trust, especially in the context of mobile payments. Traditional perspectives often view risk and trust in a binary opposition. However, findings from this study suggest that certain risks, like psychological and financial risks, can indeed foster trust. This insight necessitates a revisitation and potential expansion of existing theoretical frameworks surrounding risk and trust dynamics. Furthermore, while privacy has been positioned at the forefront of discourse surrounding digital platforms, its nuanced role in influencing trust in our study indicates the need to re-evaluate models that put an undue emphasis on privacy. Another significant theoretical takeaway is the pressing need to adapt universal technology adoption theories to encompass regional nuances, especially given the recognition of unique cultural determinants like Shariah compliance in related studies.

B. Practical Implications

From a practical standpoint, mobile payment service providers should be astute in recognizing the intricacies of perceived risks and their diverse impacts on user trust. Adopting a one-size-fits-all risk-aversion strategy might be counterproductive. Instead, discerning how specific risks can inadvertently enhance trust can offer a competitive advantage. In tandem with this, the intricate role of privacy in building trust suggests that while robust privacy measures are crucial, mobile payment platforms must also communicate other strengths to their potential users. This multifaceted approach to building trust can lead to better user retention and loyalty. Moreover, the importance of aligning services with local cultural and religious sentiments, especially in regions as diverse as Southeast Asia, cannot be overstated. Cultural alignment transcends language localization and requires an in-depth understanding and integration of regional values. Lastly, the rising trend of mobile payment adoption, especially post events like the COVID-19 pandemic, presents an opportunity for both the private and public sectors. Comprehensive awareness and education campaigns can not only educate users about potential risks but also accentuate the importance of opting for platforms that are culturally and religiously attuned to their needs.

VII. Limitations

Several constraints bound this study, warranting circumspection in interpreting the findings. Primarily, the limited dataset size could influence the derived results, making it advisable to employ larger datasets in future research. Furthermore, potential inaccuracies emanating from uncompleted questionnaires by Indonesian respondents might introduce non-statistical errors. Finally, to keep pace with evolving trends, there is room for refining the research framework, particularly by incorporating additional control variables.

References

- Aji, H. M., Berakon, I., & Md Husin, M. (2020). COVID-19 and e-wallet usage intention: A multigroup analysis between Indonesia and Malaysia. *Cogent Business & Management*, 7(1), 1804181.
- Akanfe, O., Valecha, R., & Rao, H. R. (2020). Design of

a Compliance Index for Privacy Policies: A Study of Mobile Wallet and Remittance Services. IEEE Transactions on Engineering Management.

- Alalwan, A. A., Dwivedi, Y. K., Rana, N. P. P., & Williams, M. D. (2016). Consumer adoption of mobile banking in Jordan: Examining the role of usefulness, ease of use, perceived risk and self-efficacy. *Journal of Enterprise Information Management*, 29(1), 118-139. doi:10.1108/JE IM-04-2015-0035
- Alegre, S. (2021). Protecting Freedom of Thought in the Digital Age (Cigi Policy Brief No. 165). https://www.cigio nline.org/publications/protecting-freedom-of-thought-inthe-digital-age/
- Bakri, M. H., Almansoori, K. K. S. M., & Azlan, N. S. M. (2023). Determinants intention usage of Islamic E-Wallet Among Millennials. *Global Business and Finance Review*, 28(1), 11-32. doi:10.17549/gbfr.2023.28.1.11
- Barbieri, D. M., Lou, B., Passavanti, M., Hui, C., Hoff, I., Lessa, D. A., ... Rashidi, T. H. (2021). Impact of COVID-19 pandemic on mobility in ten countries and associated perceived risk for all transport modes. *PLoS ONE*, 16(2 February), 1-18. doi:10.1371/journal.pone.0245886
- Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly: Management Information Systems*, 35(4), 1017-1041. doi:10.2307/41409971
- Caesar, A. (2021). 6 Kasus Kebocoran Data Pribadi di Indonesia. Tempo. https://nasional.tempo.co/read/150179 0/6-kasus-kebocoran-data-pribadi-di-indonesia
- Chen, C. (2013). Perceived risk, usage frequency of mobile banking services. *Managing Service Quality: An International Journal*, 23(3). doi:10.1108/MSQ-10-2012-0137
- De Kerviler, G., Demoulin, N. T. M., & Zidda, P. (2016). Adoption of in-store mobile payment: Are perceived risk and convenience the only drivers? *Journal of Retailing and Consumer Services*, *31*, 334-344.
- Featherman, M. S., Miyazaki, A. D., & Sprott, D. E. (2010). Reducing online privacy risk to facilitate e-service adoption: The influence of perceived ease of use and corporate credibility. *Journal of Services Marketing*, 24(3), 219-229.
- Ha, S. B., Udonava, I., & Cheng, M. (2021). Consumer adoption of offline M-payment: The Chinese case. *Global Business and Finance Review*, 26(2), 83-109. doi:10.17549 /gbfr.2021.26.2.83
- Hooper, D., & Coughlan, J. (2008). Evaluating Model Fit: a Synthesis of the Structural Equation Modelling Literature. *The Electronic Journal of Business Research Methods*, 6, 53-60.
- Indonesia, B. (2020). Peraturan Bank Indonesia No 22/20/Pbi/ 2020 Tentang Perlindungan Konsumen Bank Indonesia. https://www.bi.go.id/id/publikasi/peraturan/Pages/PBI_2 22020.aspx
- Irawan, D., & Affan, M. W. (2020). Pendampingan Branding Dan Packaging Umkm Ikatan Pengusaha Aisyiyah Di Kota Malang. Jurnal Pengabdian Dan Peningkatan Mutu

Masyarakat, 1(1), 32-36.

- Jang, Y. J. (2021). Building Restaurant Customers' Trust Amidst Covid-19 Crisis Through Value-and Performancebased Information: Risk Perception as a Moderator. *Global Business and Finance Review*, 26(3), 111-123. doi:10.1754 9/GBFR.2021.26.3.111
- Khatimah, H., Susanto, P., & Abdullah, N. L. (2019). Hedonic motivation and social influence on behavioral intention of e-money: The role of payment habit as a mediator. *International Journal of Entrepreneurship*, 23(1), 1-9.
- Lee, J.-M., Lee, B., & Rha, J.-Y. (2019). Determinants of mobile payment usage and the moderating effect of gender: Extending the UTAUT model with privacy risk. *International Journal of Electronic Commerce Studies*, 10(1), 43-64.
- Liébana-Cabanillas, F., Muñoz-Leiva, F., & Sánchez-Fernández, J. (2013). The impact of risk on the technological acceptance of mobile payment services. *Global Business Perspectives*, 1(4), 309-328.
- Ling, K. C., Daud, D. Bin, Piew, T. H., Keoy, K. H., & Hassan, P. (2011). Perceived risk, perceived technology, online trust for the online purchase intention in Malaysia. *International Journal of Business and Management*, 6(6), 167.
- Littler, D., & Melanthiou, D. (2006). Consumer perceptions of risk and uncertainty and the implications for behaviour towards innovative retail services: the case of internet banking. *Journal of Retailing and Consumer Services*, 13(6), 431-443. doi:10.1016/j.jretconser.2006.02.006
- Lorenzo-Seva, U., & Ferrando, P. J. (2021). Not Positive Definite Correlation Matrices in Exploratory Item Factor Analysis: Causes, Consequences and a Proposed Solution. *Structural Equation Modeling*, 28(1), 138-147. doi:10.108 0/10705511.2020.1735393
- Lubis, M., Kartiwi, M., & Zulhuda, S. (2013). A guideline to enforce privacy and data protection regulation in Indonesia. South East Asia Journal of Contemporary Business, Economic and Law, 2(3), 56-63.
- Mansoori, K. K. M. Al, & Bakri, M. H. (2023). Determinants of Disruptive Innovation That Influences Financial Service Performance. *Global Business and Finance Review*, 28(2), 69-92. doi:10.17549/gbfr.2023.28.2.69
- Marriott, H. R., & Williams, M. D. (2018). Exploring consumers perceived risk and trust for mobile shopping: A theoretical framework and empirical study. *Journal* of *Retailing and Consumer Services*, 42, 133-146. doi: 10.1016/j.jretconser.2018.01.017
- McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, 13(3), 334-359.
- Najib, M., & Fahma, F. (2020). Investigating the adoption of digital payment system through an extended technology acceptance model: An insight from the Indonesian small and medium enterprises. *International Journal on Advanced Science, Engineering and Information Technology*, 10(4),

1702-1708. doi:10.18517/ijaseit.10.4.11616

- Park, J., Amendah, E., Lee, Y., & Hyun, H. (2019). M-payment service: Interplay of perceived risk, benefit, and trust in service adoption. *Human Factors and Ergonomics in Manufacturing & Service Industries*, 29(1), 31-43. doi: 10.1002/hfm.20750
- Patil, P., Tamilmani, K., Rana, N. P., & Raghavan, V. (2020). Understanding consumer adoption of mobile payment in India: Extending Meta-UTAUT model with personal innovativeness, anxiety, trust, and grievance redressal. *International Journal of Information Management*, 54, 102144. doi:10.1016/j.ijinfomgt.2020.102144
- Phung, T. T. M., & Khuong, M. N. (2017). Personality traits, perceived risk, uncertainty, and investment performance in Vietnam. *Global Business and Finance Review*, 22(1), 67-79. doi:10.17549/gbfr.2017.22.1.67
- Purba, J. T., Samuel, S., & Budiono, S. (2021). Collaboration of digital payment usage decision in COVID-19 pandemic situation: Evidence from Indonesia. *International Journal* of Data and Network Science, 5(4), 557-568. doi: 10.5267/j.ijdns.2021.8.012
- Rabaa'i, A. A., & Zhu, X. (2021). Understanding the determinants of wearable payment adoption: An empirical study. *Interdisciplinary Journal of Information, Knowledge,* and Management, 16, 173-211. doi:10.28945/4746
- Slack, N., Singh, G., & Sharma, S. (2020). Impact of perceived value on the satisfaction of supermarket customers: developing country perspective. *International Journal of Retail and Distribution Management*, 48(11), 1235-1254. doi:10.1108/IJRDM-03-2019-0099
- Times, I. (2020). *Indonesia Milennial Report 2019*. IDN Research Institute, Indonesia.

- Tran, V. D., & Vu, Q. H. (2019). Inspecting the relationship among e-service quality, e-trust, e-customer satisfaction and behavioral intentions of online shopping customers. *Global Business and Finance Review*, 24(3), 29-42. doi:10.17549/gbfr.2019.24.3.29
- Tu, M., Wu, L., Wan, H., Ding, Z., Guo, Z., & Chen, J. (2022). The Adoption of QR Code Mobile Payment Technology During COVID-19: A Social Learning Perspective. *Frontiers in Psychology*, 12(February), 1-10. doi:10.3389/fpsyg.2021.798199
- Venkatesch, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*, 36(1), 157-178.
- Wagner, I., & Boiten, E. (2018). Privacy risk assessment: from art to science, by metrics. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology* (pp. 225-241). Springer.
- Xin, H., Techatassanasoontorn, A. A., & Tan, F. B. (2015). Antecedents of consumer trust in mobile payment adoption. *Journal of Computer Information Systems*, 55(4), 1-10.
- Yucha, N., Setiawan, S., Muttaqiin, N., Ekasari, R., & Mauladi, K. F. (2020). Digital Payment System Analysis of Buying Decision in Indonesia. *The Journal of Asian Finance, Economics and Business*, 7(10), 323-328. doi:10.13106/jaf eb.2020.vol7.n10.323
- Zuboff, S. (2019). Surveillance Capitalism and the Challenge of Collective Action. *New Labor Forum*, 28(1), 10-29. doi:10.1177/1095796018819461