Article Type: Research Paper

Determining Factors of the Perceived Security Dimensions in B2C Electronic Commerce Website: An Indonesian Study

Santos Marianus[1] and Syaiful Ali[2]

Abstract:
Research aims: This study aims to analyze the perceived security dimensions and build a research model using perceived ease of use and perceived usefulness as variables mediating the link between perceived security and the intention to use Indonesia's B2C e-commerce websites.
Design/Methodology/Approach: Using a purposive sampling approach, this study conducted an online survey of respondents who had done online transactions, such as business-to-customer (B2C) transactions.
Research Findings: The study's results showed that perceived security significantly correlated with buyers' intention to use B2C websites.
Theoretical contribution/Originality: This study contributes to developing and validating key dimensions of perceived security and their constructs. Mediation effect test results from TAM, which were perceived ease and perceived use, indicated that only the perceived usefulness variable significantly mediated the relationship between perceived security and intention to use B2C e-commerce websites. Perceived use's mediation was not supported.
Practitioner/Policy implication: This research empirically supports the perceived security construct as a second-order construct involving confidentiality, availability, non-repudiation, and privacy.
Research limitation/Implication: This study used data from Indonesian individuals, which may differ from other countries' characteristics. It may limit the research' finding generalization.
Keywords: Perceived Security; TAM; B2C; E-Commerce

AFFILIATION:
[1] P.T. T.T. Network Integration, Special Capital Region of Jakarta, Indonesia
[2] Department of Accounting, Faculty of Economics and Business, Universitas Gadjah Mada, Special Region of Yogyakarta, Indonesia

***CORRESPONDENCE:**
s.ali@ugm.ac.id

THIS ARTICLE IS AVAILABLE IN:
http://journal.umy.ac.id/index.php/ai

DOI: 10.18196/jai.v22i1.8171

CITATION:
Marianus, S., & Ali, S. (2021). factors determining the perceived security dimensions in B2C electronic commerce website usage: An Indonesian study. *Journal of Accounting and Investment*, *22*(1), 104-132.

ARTICLE HISTORY
Received:
01 Feb 2020
Revised:
15 Feb 2020
05 Dec 2020
Accepted:
21 Dec 2020

Introduction

E-commerce has become an increasingly critical alternative media for customers in meeting their shopping needs. E-commerce refers to business transactions using Internet media, websites, mobile applications, and browsers on mobile devices (Laudon & Traver, 2019). According to a Hootsuite report (2020), per January 2020, in Indonesia, there were 175.4 million internet users. This number increased by 17% or 25 million users compared to 2019. Furthermore, Hootsuite reported that Internet penetration in Indonesia in January 2020 was 65% of Indonesia's total population. In terms of mobile connections, as of January 2020, Indonesia had 338.2 million connections, an increase of 4.6% compared to 2019.

The number of mobile connections was equivalent to 124% of the total population in Indonesia. These data revealed that Internet media and applications on mobile devices in Indonesia could support the development of e-commerce in Indonesia very quickly. It is supported by data from e-commerce users in Indonesia, estimated to have reached 168.3 million users in 2019 (Statista, 2019) and is projected to increase to 212.2 million users in 2023. In terms of e-commerce penetration rates in Indonesia, the data demonstrated a high increase. In 2023, it is estimated that it will reach 75.3% of the total population (Statista, 2019).

The increase in popularity of online shopping is paralleled with an increase in concern regarding internet security. A study conducted by Matic and Vojvodic (2014) revealed that concern mainly with security had caused consumers to avoid shopping online. A recent study by Balapour, Nikkhah, and Sabherwal (2020), in the context of mobile app users' security perceptions, showed that perceived privacy risk negatively influenced users' security perceptions. Another recent study carried out by Oni and Adeyeye (2020) found that B2C customers' satisfaction was positively affected by their perceived security. These studies showed that perceived security played a critical role when consumers perform B2C transactions. As a result, e-commerce providers must manage threats to their B2C websites and increase consumers' perception towards B2C safety (Fang, Qureshi, Sun, McCole, Ramsey, & Lim, 2014).

Despite the importance of the perceived security factor in B2C, a literature review regarding perceived security has uncovered inconsistent conceptualization of perceived security in empirical studies. Several studies (Bodin, Gordon, & Loeb, 2005; Siponen & Oinas-Kukkonen, 2007; Cegielski, 2008; Parent, 2007; Gurbani & McGee, 2007) indicate that practitioners of information system and researchers, in general, agree that security is a multi-dimensional construct based on several dimensions (for example, confidentiality, integrity, availability, non-repudiation, authentication, and privacy). However, many of these empirical studies have not studied the factors that can mediate perceived security's multidimensionality (Hartono, Holsapple, Kim, Na, & Simpson, 2014). Previous empirical studies ignored multidimensionality from perceived security (Ryan & Ryan, 2005; Erlich & Zviran, 2010; Gordon, Loeb, & Zhou, 2011).

Apart from validating the dimensions of perceived security, this study empirically examined the importance of perceived security's role in using B2C e-commerce websites. Based on the above phenomenon, the researchers formulated the following research questions: (1) does perceive security (confidentiality, non-repudiation, integrity, availability, privacy, and authentication) influence buyers' intention to use B2C websites? (2) can the perceived ease of use and perceived usefulness mediate the relationship between perceived security and buyers' intention to use a B2C website? The difference of this research with previous research is to examine perceived security from a multi-dimensional aspect. The inclusion of other dimensions (i.e., availability, confidentiality, non-repudiation, and privacy) reassures that a perceived security construct is consistent with previous studies.

Literature Review and Hypotheses Development

Numerous studies related to perceived security stem from the Technology Acceptance Model (TAM) introduced by Davis (1989). This study investigates the impact of customer perceived security towards their intention to purchase via B2C websites by incorporating perceived ease of use and perceived usefulness of customers as mediating factors in that relationship (Hartono et al., 2014). As this study examines the acceptance of e-commerce, the research model is based on the Technology Acceptance Model by Venkatesh and Davis (2000). The research introduced by Venkatesh and Davis (2000) does not include the "attitude towards using" construct as a development of the Davis Model (1989).

The TAM introduced by Davis (1989) is a customer acceptance model to form an information system with three constructs, namely attitude towards using, intention to use, and actual usage. According to Davis (1989), attitude towards using describes individuals' positive or negative feelings in conducting specific activities. TAM predicts how users respond to new technologies (Salisbury, Pearson, Pearson, & Miller, 2001). Salisbury et al. (2001) examined the effect of perceived security and when and how new technology was used. Their research was conducted by constructing a measurement scale of perceived web security and applying that scale to investigate the impacts of buyers' intention to use B2C e-commerce websites. Further, the study also examined the effect of perceived ease of use and perceived usefulness towards online shopping, and the interest in buying products through B2C websites. Their study found a positive association between the level of perceived web security and interest in buying products via B2C websites.

Trust is a primary factor in the process of e-commerce. Trust relates to the correlation between seller and buyer and even third parties. In McKnight and Chervany's study (2001), the term "trust" indicates belief or trust. This term refers to the belief that someone relies on a promise made by someone else and that others, in unexpected situations, will act towards themselves in the name of goodwill. Customer trust will increase if suppliers exhibit behavior similar to previous encounters (McKnight & Chervany, 2001).

Mayer, Davis, and Schoorman (1995), McKnighy and Chervany (2001) mentioned that trust has three characteristics: competence, virtue, and integrity. Gefen (2000) expressed that commerce with suppliers involving the customer in an uncertain situation hampers their interest in conducting commerce at all. Trust is crucial when uncertainty and risk are inherent to the contract, and collateral is often ignored (Crosby, Evans, & Cowles, 1990; Grazioli & Jarvenpaa, 2000). The e-commerce environment possesses all these characteristics.

Furthermore, studies on the role of perceived security in B2C have connected perceived security to perceived trust (for example, Gefen, 2000; Gefen, Karahanna, & Straub, 2003) and perceived risk (for example, Bhatnagar, Misra & Rao, 2000). Cheung and Lee (2001) have also investigated the impact of security and trust in the context of B2C e-

commerce. These studies suggested that perceived security, with other factors such as trust, significantly impacted consumers' trust when shopping online. Flavián and Guinalíu (2006) confirmed these results by showing that increased customer B2C website perceived security would result in higher website trust and loyalty. A study by Kim, Ferrin, and Rao (2008) showed that perceived security and other factors are essential antecedents of trust and perceived risk. From the studies mentioned above, it can be concluded that trust holds a critical role in e-commerce.

Although prior studies have incorporated two most frequently used variables: trust and perceived risk (Kim et al., 2008), those studies only used variables derived from the conceptual framework of TAM (perceived ease of use and perceived usefulness) based on keeping a brief survey so that the response rate was high. The numerous questions in the survey would make respondents unwilling to fill out the questionnaire. However, this study employed the TAM conceptual framework variables as the relationship between perceived security. The various constructs outside of TAM (for example, trust and perceived risk) have been well established (Hartono et al., 2014). Therefore, this research examines perceived security from multi-dimensional aspects and the inclusion of other dimensions (i.e., availability, confidentiality, non-repudiation, and privacy) and reassures that a perceived security construct is consistent with previous studies.

Hartono et al. (2014) have classified and specified the dimensions of perceived security by looking at the four most significant dimensions from various previous studies, namely (non-repudiation, confidentiality, integrity, and availability). Definitions about perceived security reflect comprehensive studies on the definition in the information system and other relevant sciences (for example, computer science) (for example, Salisbury et al., 2001: Cheng, Lam, & Yeung, 2006; Chellappa & Pavlou, 2002; Fang et al., 2006; Yousafzai, Pallister & Foxhall, 2009; Kim, Tao, Shin, & Kim, 2010). Moreover, these studies have observed literature that discusses security issues, including perceived security and actual security. The study's findings found that confidentiality, integrity, and availability were frequently used in the early stages. Gurbani and McGee's (2007) study has added non-repudiation, authentication, access controls, secured communication, and privacy to the perceived security construct.

Azizi and Javidani (2010) assume that financial information security, such as credit card information or online bank account passwords, is the key problem with e-commerce security. Chellappa and Pavlou (2002) contended that online transactions are secure when information from one point to another is not read and changed without a valid authorization or lost during transmission. Kurt and Hacioglu (2010) suggested that online protection is an ethical problem for consumers and that they expect online vendors to ensure the confidential security details they carry.

Several studies, such as that conducted by Siponen and Oinas-Kukkonen (2007), have shown that the word “security” is commonly used. However, others have been more rigorous and precise in the use of the term. Some studies have used appropriate security measures as a different technology by deciding the essence and implementation of technical safety, authentication, and encryption, or internal or external factors that

provide confidentiality assurance, such as anonymity, security declaration, and privacy policy solution. For this reason, there are also two key security measures other than the broad meaning of the word “security”: confidentiality and privacy.

Further, Chellappa and Pavlou (2002) examined the effect of perception on various factors, including encryption, authentication, technical protection, and verification of customer perceived security on consumers. Similarly, Kim et al. (2010) analyzed the effect of customer perception from security statements and technical protection sites on their perceived security as a whole. Belanger, Hiller, and Smith (2002) used six factors: privacy, availability, non-repudiation, confidentiality, integrity, and authentication to measure customer perception and trust of the vendor's worthiness. Their study found that customer value security was more significant than other variables in building trust towards their intention to use websites. Therefore, it can be concluded that customers' perception of perceived security is entirely different from their perception of certain confidentiality factors, such as third-party assurance or security/privacy statement. From several literature sources and inconsistencies in studies related to perceived security dimensions, a research model could be built based on hypothesis development shown in Figure 1.

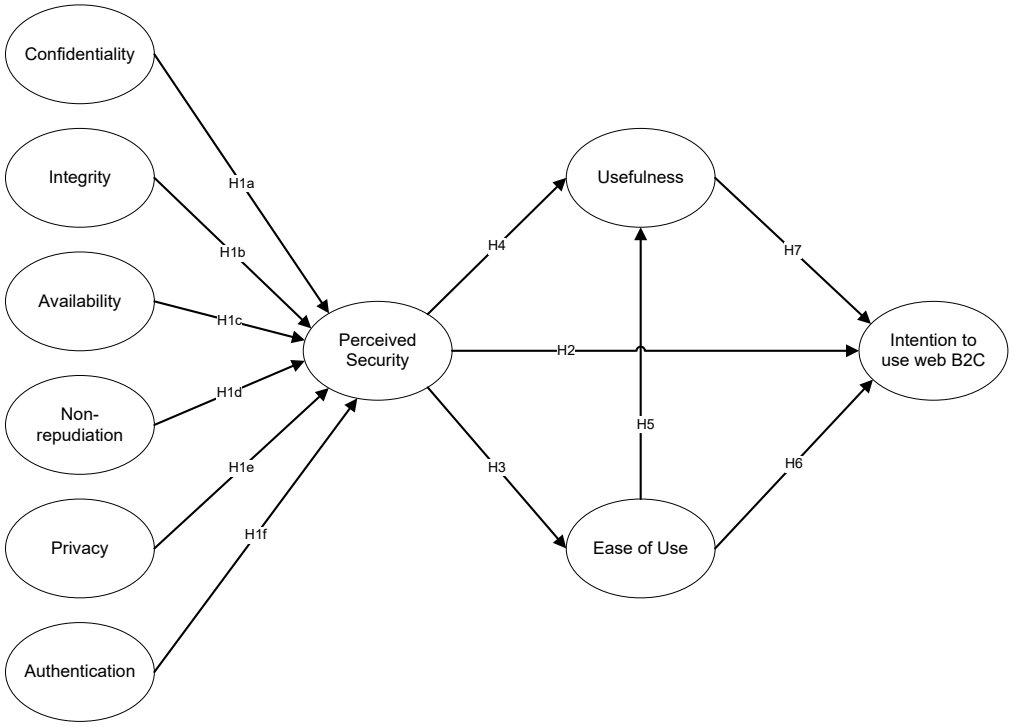

Figure 1 Research Model

Previous studies (Ryan & Ryan 2005; Erlich & Zviran 2010; Ransbotham, Mitra, & Ramsey, 2012) have agreed that perceived confidentiality is one of the most critical dimensions of perceived security. Turban, King, Lee, Liang, and Turban (2010) briefly defined the principle of confidentiality as a guarantee of private data and accuracy. A system with a higher priority towards confidentiality can better anticipate and mitigate

false disclosures of information, for example, information leakage, thus establishing the system's security (Tsiakis & Sthephanides, (2005).

A typical measurement of security to maintain confidentiality is, for example, data encryption. The encryption creates the presumption that sellers who maintain a system with priority on consumer data confidentiality will make the consumers more comfortable conducting the transaction. Subsequently, a hypothesis was formulated as follows:

***H_{1a}**: Perceived confidentiality correlates positively with perceived security.*

Integrity is one of the most critical dimensions of perceived security (Hartono et al., 2014; Vaidyanathan & Mautone, 2009; Cegielski, 2008). Turban et al. (2010) expressed that integrity ensures that data is accurate, and no portion of the message is modified. Integrity can also mean that payment data cannot be damaged, both deliberately and accidentally. The higher the assurance in integrity that the selling company can provide, the higher the feeling of security felt by consumers when conducting transactions with that company. They are assured that the company will never modify their data illegally. Subsequently, a hypothesis was formally stated as follows:

***H_{1b}**: Perceived integrity correlates positively with perceived security.*

One of the most critical dimensions in perceived security expressed by Hartono et al. (2014) is availability. This last dimension relates to how information access is opened to consumers authorized for such information. Availability refers to how far information is available for the authorized subject if needed (Tsiakis & Sthephanides, 2005). A system with a superior availability can consistently provide relevant information to the authorized party. The less the information is available for consumers, the less the feeling of security within the buyers, which in turn will cause them to be reluctant to use websites to conduct transactions. Subsequently, a hypothesis was formulated as follows:

***H_{1c}**: Perceived availability correlates positively with perceived security.*

Non-repudiation is revealed to be one of the critical dimensions of perceived security (Turban et al., 2010; Hartono et al., 2014). It relates to the exchange/transaction between buyer and seller, particularly to the system's ability to guarantee that the person who claims to be the seller received information that has been sent by the buyer. Non-repudiation ensures that the seller cannot deny the transaction's completion (Siponen & Oinas-Kukkoken, 2007).

Consumers will feel safe in transacting with the knowledge that one party, the vendor, cannot cancel the transaction they are conducting. The presence of a non-repudiation guarantee is predicted to increase the feeling of security in transacting through

websites. A digital signature is one of the measurements of security commonly used to maintain non-repudiation. Subsequently, a hypothesis was formulated as follows:

***H_{1d}**: Perceived non-repudiation correlates positively with perceived security.*

Research conducted by Hole, Tjϕstheim, Moen, Netland, Espelid, and Klingsheim (2008) proposed that privacy is often defined similarly to confidentiality. However, these two are different terms. Furthermore, Bella, Giustolisi, and Riccobene (2011) found two paradigms about privacy in e-commerce. The first paradigm relates to the trust to conduct transactions online, and the second is associated with the anonymity or the use of a pseudonym in transacting to protect privacy. Despite that, studies conducted by Ryan and Ryan (2005), Erlich and Zviran (2010); Berghmans and Van Roy (2011) did not find any dimension of privacy that is one of the dimensions of perceived security. The researchers suspect these conflicting findings stem from the researchers' perspective, who view privacy as unity with perceived confidentiality. For that reason, this study is predicted to support the findings of Bella et al. (2011) and Hole et al. (2008) by proposing the following hypothesis:

***H_{1e}**: Privacy correlates positively with perceived security.*

Studies conducted by Ransbotham et al. (2012), Siponen and Oinas-Kukkonen (2007), Hartono et al. (2014) did not find authentication to have any impact on perceived security. However, Cegielski (2008), Vaidyanathan and Mautone (2009), Turban et al. (2010) expressed that authentication had some correlation with perceived security. Authentication is a process of a transaction's identification. Both parties must be identified well as the customer responsible for paying and the vendor responsible for providing the product and service (Turban et al., 2010). With this feature, a customer will feel safe knowing that they are transacting with a vendor already identified. Companies implementing authentication in their every transaction will increase their customers' perceived security, which increases their willingness to use the company website to transact. Subsequently, a hypothesis was formally formulated as follows:

***H_{1f}**: Authentication correlates positively with perceived security.*

Internet-based commerce carries an inherent risk from the perspective of security. The increased uncertainty in e-commerce results from the parties conducting a transaction in different places and cannot rely on physical intimacy, handshakes, and gestures (Clarke, 1998). One of the parties can also not directly monitor the other party's actions (Grazioli & Jarvenpaa, 2000).

Consequently, the security network is often absent in the e-commerce environment. If individuals in various nations conduct e-commerce transactions, they may not abide by the laws in both transacting countries (Clarke, 1998). Internet vendor security is the

primary factor affecting the growth of e-commerce (Bhatnagar et al., 2000; Gefen, 2000). Companies with priority on security for their customers in conducting transactions are predicted to increase the customers' interest always to use the company's website. Subsequently, a hypothesis was formulated as follows:

***H_2**: Perceived security correlates positively with interest in using B2C e-commerce websites.*

A study conducted by Lu, Lai, and Cheng (2007) proposed that perceived security positively correlated with perceived ease of use. Usoro, Shoyelu, and Koufie (2010) stated that perceived ease of use encompasses individual comfort in using the system. The higher the perceived security, the higher the customers' comfort to use the system ought to be. Subsequently, a hypothesis was formulated as follows:

***H_3**: Perceived security correlates positively with perceived ease of use.*

Gefen, Karahanna, and Straub (2003) said that an e-commerce application's usefulness is distinguished between short-term and long-term usefulness. Long-term usefulness, for example, is the ability of a site to protect its customers from spending additional expenses due to a security breach (access which is not authorized/the use of their credit card by other parties). An increase in perceived security in an e-commerce website will increase consumer confidence that the website they are using will benefit them in the long run. Although there has not been any study directly connecting perceived security and perceived usefulness to the researchers' best knowledge, a positive correlation between them seems logical. Subsequently, a hypothesis was formulated as follows:

***H_4**: Perceived security correlates positively with perceived usefulness.*

TAM's use with the construction of additional perceived web security dimensions carried out by Cheng et al. (2006) also displayed that perceived web security, along with perceived ease of use and perceived usefulness, significantly correlated to the use of online banking websites. Lian and Lin (2008) exhibited that perceived security, along with individual innovation, concern towards individual privacy, an involvement of individual product, product, and type of service, were all essential determining factors of online shopping behavior. Chang and Chen (2009) found that customer satisfaction on B2C websites was determined by perceived security and quality. The two variables correlated positively with customer intentions to use a B2C website.

This research seeks to expand the flow of research in perceived security in the context of B2C, which is by theoretically studying TAM as variables mediating perceived security and the intention to use B2C websites, which are perceived ease of use and perceived usefulness. For that reason, the hypotheses proposed are as follows:

***H_5**: Perceived ease of use correlates positively with perceived use.*

***H_6**: Perceived ease of use correlates positively to the intention to use B2C e-commerce websites.*

***H_7**: Perceived usefulness correlates positively to the intention to use B2C e-commerce websites.*

Research Method

The population used for this research was the people using B2C websites to conduct e-commerce in Indonesia. This research used "purposive sampling". This sampling method implementation was done by collecting samples from respondents from a network reference (Hartono et al., 2014). This decision was made based on the assumption that respondents were familiar with or had previously done online transactions, such as Business-to-Customer (B2C). The target sample to participate in this research was 320 participants.

"Purposive sampling" was employed to collect data and sample selection. Other published researchers have used this method (Mitchell, 2006; Keil, Lee, & Deng, 2013; Kiang, Ye, Hao, Chen, & Li, 2011). Purposive sampling was done by taking a sample from a population-based on specific criteria. This research used the following criteria: students who took a course in e-business or often conducted transactions online, and practitioners of online commerce who conducted e-commerce in a B2C manner. For practitioners, commerce could be identified via facebook.com and Blackberry Messenger (BBM). This research sample consisted of three groups: business program undergraduate students, graduate students, and practitioners of e-commerce. The data collection method was conducted by two methods: online (web-based) survey and mail survey.

An online web-based questionnaire was created using an application from docs.google.com. Respondents were invited by email, BBM, Facebook, with messages containing links connected to the website containing the questions in the questionnaires, and subsequently, fill them in. For undergraduate students, the requirement was that they had taken a course in e-business. The researchers expected many of the online customers to know the critical aspects of online security. A total of 300 participants from this research were anticipated to fulfill the requirements to participate in this research. To address the non-response bias issue, this study compared the early responses with the later responses. The absence of difference between these suggests no non-response bias (Hair, Black, Babin Anderson, & Tatham, 2006).

The perceived security dimension construct that is entirely different is determined by the composite that forms perceived security, not only a reflection or manifestation of perceived security. For that reason, a perceived security model must be constructed as a multi-dimensional construct (Diamantopoulos, Riefler, & Roth, 2008). This research's

specific measurement model was the guide to develop a formative index, as recommended by Diamantopoulos and Winklhofer (2001). The first step was the domain's specification. In this step, the meaning of the language was reviewed as the basis of determining the perceived security's conceptual domain, including relevant definitions and dimensions. Next, to specify every dimension of perceived security, a literature review was performed to classify and generate reflective indicators for every construct's dimension.

The third step was the validation of indicators. In this step, reflective indicators were validated as valid dimensions by assessing the external validity and its multicollinearity. The fourth step involved validating security considered the second-order format, with relevant dimensions as first-order reflective factors. Subsequently, another guidance was to combine and construct perceived security measurements into the traditional statistical analysis (Hartono et al., 2014).

The dimensions removed due to inconsistency with perceived security were authentication, control access, and communication security (Hartono et al., 2014). These dimensions are considered as representing the measurement of information assets protection. Further, privacy was also removed as previous researchers considered conceptualizing it as a separate thing from the perceived security construct (Flavián & Guinalíu, 2006; Roca, Garcia, & de la Vega, 2009; Yousafzai et al., 2009). However, in this research, all three dimensions of perceived security were tested again to identify the significance and correlation towards perceived security in Indonesia's context (Cegielski, 2008).

Based on the six-dimension framework, security measures were developed: perceived confidentiality, perceived integrity, perceived availability, perceived non-repudiation, privacy, and authentication. Security operationalization was considered to be a second-order format, not a reflective form, consistent with the four criteria recommended by Jarvis et al. (2003). First, the dimensions define characteristics of security manifestation that is felt. How much belief the online buyer has that the transaction conducted with the online vendor is safe (i.e., perceived security) is marked by (a) how much belief the customer has that transaction information will not be disclosed (i.e., perceived confidentiality breach) or modified by unauthorized parties (i.e., perceived integrity violation), (b) how much information the online vendor is able and willing to produce for the authorized customer if needed (i.e., perceived availability), and (c) how much the online vendor can claim and cannot deny that a transaction is completed (i.e., perceived non-repudiation) (Jarvis et al., 2003).

Second, the level of perceived security will be affected by changes in one dimension, but perceived security changes will not necessarily affect all dimensions. For instance, if an online transaction is interrupted by system failure (i.e., a decrease in perceived availability), the customer's perceived security will also decrease. A decrease in perceived security, however, will not cause a decrease in perceived availability (Hartono et al., 2014).

Third, every dimension is a different concept. The definition of that dimension represents six different constructs, each impacting independently on perceived security. Fourth, the orthogonal dimension and a change in one dimension will not cause a change in other dimensions. For example, customer transaction is disrupted, creating a decrease in the system available to the customer. However, perceived confidentiality, integrity, and non-repudiation are not always affected. An empirical multicollinearity study will allow us to test this assumption (Jarvis et al., 2003).

Consistent with Anderson and Gerbing's (1988) work, measurement evaluation reflects dimensions for content validity of the perceived security, reliability construction, convergent validity, and discriminant validity. Content validity was established by a group of potential respondents and experts through a repeated process of reviewing and revising construct items in questionnaires. Initially, to evaluate constructs, a list of potential indicators was made. A pre-test was then carried out towards these constructs with a group of graduate students majoring in information systems and related lecturers. This initial testing aimed to clarify construct items, relevance, and clarity of the meanings. The reviewer's comments were used to revise relevant items. When all reviewers were pleased, this evaluation process was replicated, and no further changes were recommended.

In this research, each construct was measured through several question items. This survey requested that the respondents assessed how much they agreed with the question items' claim. All indicators were measured on a Likert Seven-point Scale. Number 1 represented the respondent's opinion as "strongly disagree," and number 7 as "strongly agree". The question items in this research were adapted from a study by Hartono et al. (2014) and Cegielski (2008) with translation into Indonesian. Aside from that, the data quality needed to be tested to identify whether the respondents were genuinely willing to fill in the questionnaire. For that reason, to ensure that the questionnaire items were sufficient, correct, and can be understood, they needed to be tested (Hartono, 2008). Instrument testing was done by doing a pre-test on master program students.

This study conducted validity and reliability testing before conducting hypothesis testing. A validity test was done on every question item in every variable. Confirmatory Factor Analysis (CFA) was used to identify the validity of each question item. Furthermore, Partial Least Square (PLS) was chosen for this research due to the lack of need to load the samples and the fact that the sample was free distribution. Research conducted by Hair, Black, Babin, and Anderson (2010) and Hartono (2008) presented those question items that are certain construct indicators must correlate with themselves (i.e., convergent validity). It must follow three criteria: (Fornell & Larcker, 1981): (1). Every loading factor item must be significant and is > 0.70; (2). Combined reliability (ρc) > 0.80; (3). Average Variance Extracted (AVE) > 0.50 or square root of AVE must be > 0.71.

A reliability test was needed to identify whether there was consistency in the measurement results if the measurement were to be done more than once against the

same symptoms and with the same measurement tools. The reliability test was done with a measurement that fulfilled the criteria of composite reliability above 0.70. The reliability test could also be done by calculating each item's Cronbach Alpha in a variable with a value higher than 0.60.

Hypotheses were tested using Structural Equation Modelling (SEM) with a statistical tool WarpPLS (Anderson & Gerbing, 1988; Bagozzi & Yi, 1988). Partial Least Square (PLS) was chosen because the size of the sample was not very big. Also, this research was aimed to develop a model (Sholihin & Ratmono, 2013). The structural model was evaluated by looking at the results of path coefficient estimates and their significances.

Result and Discussion

Table 1 shows the demographic profile of the respondents. Instrument testing in this research was the most critical part. Research data would not be used if the measurement instruments used did not have high validity and reliability because hypothesis testing is profoundly influenced by data quality (Cooper and Schindler, 2006). Before the primary survey, two pre-survey stages (pre-test and pilot-test) were conducted to identify face validity, content validity, and initial reliability of the available instruments.

Table 1 Demographic profile of the respondents

Demographic profile of the respondents			
Demographic Variable		**Frequency**	**%**
Gender	Female	167	56
	Male	131	44
	Missing	2	1
Age	<20	86	29
	<30	167	56
	<40	42	14
	<50	3	1
	<=50	0	0
	Missing	2	1
Occupation	Housewife	43	14
	Student	118	39
	Office Worker	47	16
	Self-employed	69	23
	Others	21	7
	Missing	2	1
Education	Below high school	8	3
	High school	68	23
	College student	143	48
	College graduate or over	73	24
	Missing	8	3

In the early stages of data analysis, a pre-test was done to test the face validity. There was a common understanding between the authors and respondents with regards to the questionnaire content. The purpose of the pre-test was also to test content validity. In

this research, the pre-test was done in three stages. Firstly, the instruments were initially tested by gathering the opinion of graduate student colleagues at Universitas Gadjah Mada to obtain an appropriate sentence structure. Secondly, revision recommendations were implemented in the second version. Thirdly, the items that had been tested were included in the pilot test phase to be tested in a small sample of 32 respondents.

After the pre-test was conducted, a pilot test was carried out to detect any weaknesses in the questionnaire to ensure that the questionnaire used in this research was valid and reliable in measuring the hypothesized variables. A pilot test could be done on 10-30 respondents (Jogiyanto, 2008). In this research, the pilot test was done on 32 respondents, including students in a master's program. The pilot test's first aim was to ensure that the questionnaire's items were sufficient, correct, and understood. The pilot test's second aim was to obtain an initial assessment of the scale's reliability (Hartono, 2008).

Data from the test results were analyzed using the WarpPLS version 3.0 software. These test results indicated that these research instruments' construct validity was sufficient as the loading factor values of the items used to measure constructs fulfilled the minimum standard (loading > 0.70). However, a factor loading of 0.59 was still supported, which was the authentication construct. Moreover, reliability tests also showed that the instruments used were reliable, evident from the composite reliability values, and Cronbach's Alpha higher than 0.60. Overall, the instruments tested did not indicate any significant changes and could be used in this research.

Table A1 in the Appendix displays that convergent validity for confidentiality variable (CONF), integrity (INT), availability (AVA), non-repudiation (REP), and privacy (PRIV) have been fulfilled with loading factors higher than 0.70 and were significant (p values < 0.05). Indicators with the highest loading factor values were present in INT2 with a value of 0.896. However, two indicators, AUT1 and AUT2, exhibited loading factors lower than 0.70, with values of 0.681 and 0.633.

Table 2 Correlation Values between Latent Variables

	CONF	INT	AVA	REPU	PRIV	AUT	SEC	INTUSE	EOU	USE
CONF	**0.864**									
INT	0.498	**0.873**								
AVA	0.585	0.242	**0.866**							
REPU	0.499	0.430	0.398	**0.85**						
PRIV	0.526	0.535	0.448	0.462	**0.854**					
AUT	-0.031	-0.076	-0.153	0.004	0.063	**0.69**				
SEC	0.342	0.570	0.376	0.343	0.375	-0.038	**0.785**			
INTUSE	0.111	0.078	0.078	0.151	0.157	-0.008	0.157	**0.721**		
EOU	0.412	0.431	0.428	0.402	0.369	0.038	0.439	0.202	**0.805**	
USE	0.411	0.462	0.441	0.385	0.509	0.026	0.419	0.166	0.275	**0.861**

Note: Square roots of average variances extracted (AVE's) shown on diagonal.

Discriminant validity could be measured by the Average Variance Extracted (AVE) value. Discriminant validity can be considered sufficient if each variable's AVE value exceeds

0.70 (Hair et al. 2010). A discriminant variable can be seen by creating a comparison between the AVE value of each construct and the correlation between constructs. If AVE's square root is higher than the correlation with other constructs, the model can be declared sufficiently valid. Table 2 shows the AVE's square root values and each latent variable's correlation values to test the discriminant variable (Hair et al. 2010). Table 1 reveals that the variables confidentiality, integrity, availability, non-repudiation, and privacy fulfilled the AVE criterion, with the highest value being integrity, at 0.873. However, the authentication variable did not meet the AVE criterion because it was below the criterion, with 0.690.

The consistency of an instrument can be measured by using Cronbach's Alpha and Composite Reliability. Both of these measurements have different roles. Cronbach's alpha is to measure the lower limit of reliability of a construct. In contrast, composite reliability measures the actual value of a construct. Research done by Hair et al. (2010) reveals that a construct is considered reliable if it has a Cronbach's alpha and composite reliability greater than 0.70.

Table 3 Latent Variable Coefficients

	CONF	INT	AVA	REPU	PRIV	AUT	SEC	INTUSE	EOU	USE
Composite reliability	0.898	0.905	0.90	0.886	0.89	0.731	0.865	0.763	0.845	0.896
Cronbach's alpha	0.83	0.843	0.833	0.807	0.814	0.449	0.791	0.735	0.722	0.826
AVE	0.746	0.762	0.75	0.722	0.729	0.477	0.616	0.749	0.749	0.742

Table 3 conveys that variable confidentiality, integrity, availability, non-repudiation, and privacy fulfilled the Cronbach's Alpha and composite reliability criteria of greater than 0.70. However, the authentication variable had not fulfilled these criteria, so this variable was removed from further analysis. The removal is consistent with the findings of Hartono et al. (2014) that suggested that authentication is not one of the indicators used to measure perceived security but rather an attempt to prevent attacks on a system.

In this research, a dependent variable of perceived security was a second-order construct, with five indicators: confidentiality, integrity, availability, non-repudiation, and privacy. To estimate the structural model, perceived security, namely a second-order construct, had to be measured using latent variable scores/factor scores from the five dimensions (confidentiality, integrity, availability, non-repudiation, and privacy). However, before analyzing the inner model, the outer model had to be evaluated for the perceived security construct and intention to use B2C e-commerce websites.

The criteria for evaluating the outer model of the perceived security and intention to use B2C websites formative constructs is that each indicator must obtain a significant value (value $p < 0.05$), and no multicollinearity exists (VIF < 2.5). For that reason, looking at the indicator weight test results from Table A2 is needed (see attachments in Appendix).

Table A2 shows that the perceived security formative construct, with its five indicators, obtained VIF values: lv_CONF (2.244), lv_INT (2.026), lv_AVA (2.289), lv_REPU (1.452), and lv_PRIV (1.593), and thus fulfilling the VIF criterion with a p-value < 0.01. Similarly, the intention to use the B2C websites construct, with its three indicators, obtained VIF values: INTUSE1 (1.108), INTUSE2 (1.143), and INTUSE3 (1.195) at a p significant value of < 0.01. These results indicated that perceived security and intention to use B2C websites did not contain multicollinearity in each of their indicators and had fulfilled the validity requirements of formative constructs.

To evaluate whether the model is suitable or supported, the Average Path Coefficient (APC), Average R-squared (ARS), and Average Variance Inflation Factor (AVIF) can be used. The p-value for APC and ARS must be smaller than 0.05, or in other words, significant. Furthermore, AVIF, as a multicollinearity indicator, must be smaller than 5.

Table 4 Model Fit Index and P-Value

	Model Fit Indices	P Values
Average Path Coefficient (APC)	0.258	P < 0.01
Average R-Squared (ARS)	0.53	P < 0.01
Average Variance Inflation Factor (AVIF)	2.26	Good if < 5

From Table 4, it can be seen that the "goodness of fit model" criteria had been fulfilled, with an APC value of 0.258 and ARS value of 0.530 and significantly (p < 0.01). The AVIF value had also fulfilled the criterion, with a value of 2.260, which was smaller than 5.

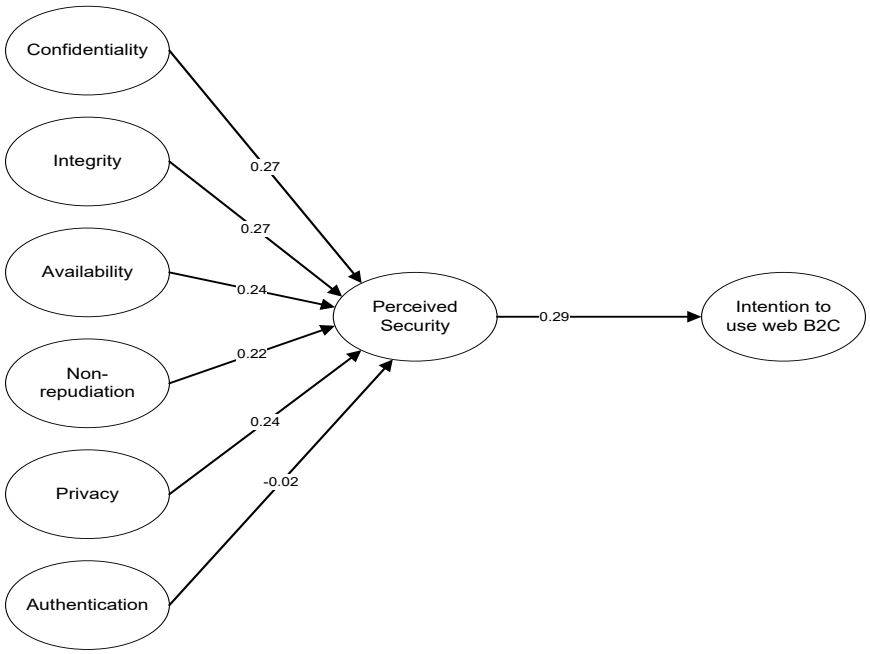

Figure 2 Research Model before Mediating Variables

The relationship between perceived security and intention to use B2C websites was statistically significant, with a coefficient of 0.25 and a p-value < 0.01. The result suggested that perceived security correlated positively to use B2C websites or, in other words, the higher the perceived security, the higher the intention to use B2C e-commerce websites.

Perceived security (SECURITY) obtained an R-square of 0.99. The result indicated that 99% of the variable perceived security could be explained by confidentiality (CONF), integrity (INT), availability (AVA), non-repudiation (REP), and privacy (PRIV). Figure 2 shows that the intention to use B2C e-commerce websites (INTUSE) had an R-square of 0.06. This value indicated that perceived security could explain 6% of the variable intention to use B2C websites. In other words, the other 94% of the variables, which could influence the intention to use B2C e-commerce websites, consisted of variables other than perceived security.

Intention to use B2C websites (INTUSE) obtained an R-square of 0.06. The result signified that perceived security could explain 6% of intention to use B2C e-commerce websites. It indicated that there were still other variables outside of perceived security that made up the other 94%. Research conducted by Hartono et al. (2014) found that perceived security could be mediated by the variables perceived ease of use (EOU) and perceived usefulness (USE). For that reason, this research used variables perceived ease of use (EOU) and perceived usefulness (USE) as mediating variables.

Research done by Hartono et al. (2014) proposed that perceived security could be mediated by the variables' ease of use and usefulness. For that reason, this research also tested the mediating effect of these two variables. Figure 3 below displays the effect of mediation by the ease of use and usefulness on the intention to use websites.

Test results for the model with the mediating variable perceived ease of use and perceived usefulness in Figure 3 exhibit how perceived ease of use fully mediated the relationship between perceived security and intention to use B2C e-commerce websites. It could be seen from the change in the coefficient and p-value. Figure 3 displays a significant relationship between perceived security and intention to use B2C websites (coefficient = 0.25 and P < 0.01). However, after including the mediating variables (ease of use and usefulness), the coefficient of the direct relationship of perceived security from 0.25 with a p-value of 0.01 to an insignificant value of 0.19 and p-value 0.15. It illustrated that other variables could explain the intention to use B2C websites outside of perceived security. First, perceived security (SECURITY) did have direct impact on intention to use B2C websites (INTUSE) (coefficient = 0.19 and p-value = 0.15).

Test results on Figure 3 suggest that perceived security had a direct impact on perceived usefulness (coefficient = 0.64 and p-value < 0.01), and ease of use also had a significant influence on intention to use B2C e-commerce websites (coefficient = 0.17 and p-value < 0.05). In other words, ease of use mediated the relationship between perceived security and intention to use B2C websites.

Test results using statistics also exposed that perceived security had effect on perceived usefulness (coefficient = 0.21; $p < 0.01$), but usefulness had no significant effect on intention to use B2C websites (coefficient = 0.05; $p < 0.33$). For that reason, hypothesis 4 (security correlates positively with usefulness) was supported. However, hypothesis 5 (usefulness correlates positively to use websites) was not supported. Hypothesis 6, which states that ease of use correlates positively with usefulness, was supported (coefficient = 0.64; $p < 0.01$).

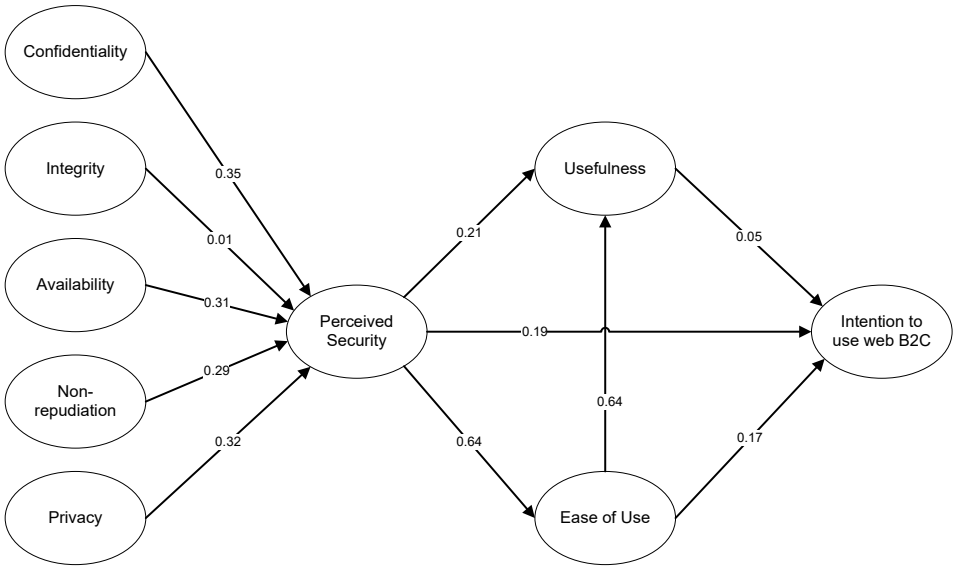

Figure 3 Research Model after Mediated by Ease of Use and Usefulness

Statistical results in Figure 3 also show that when ease of use (EOU) and usefulness (USE) was included in the research model, the direct effect of perceived security on the intention to use B2C websites became insignificant (p-value = 0.15). Overall, these results revealed that perceived ease of use (EOU) mediated fully the effect of perceived security on the intention to use B2C e-commerce websites. It corresponds to Podsakoff and Organ's (1986) argument that full mediation occurs when a significant direct effect turns into an insignificant effect after controlling the effect of mediating variables (Sholihin & Ratmono, 2013). Table 5 shows values from an indirect effect.

Table 5 shows that an indirect effect of 0.485 and its largest proportion could be attributed to EOU.

Table 5 Indirect Effect

SEC- USE-INTUSE Route	0,21 x 0,05	0.0105
SEC-EOU-USE-INTUSE Route	0.64 x 0.64 x 0.05	0.02048
SEC- EOU-INTUSE Route	0.64 x 0.71	0.4544
Indirect Effect		0.48538
Direct Effect		0.02048
Total Effect		0.50586

Table 6 Model fit Indices and P values

	Model Fit Indices	P Values
Average Path Coefficient (APC)	0.291	P < 0.001
Average R-Squared (ARS)	0.536	P < 0.001
Average Variance Inflation Factor (AVIF)	1.932	Good if < 5

Output indices in Table 6 suggest that all three fit indicators (perceived security, perceived ease of use, perceived usefulness) had fulfilled the criteria. The APC and ARS values were significant ($p < 0.001$) and AVIF < 5. It showed that the model proposed was supported by the data.

Hypothesis 1a stated that confidentiality had a positive correlation with perceived security. This presumption is also based on the findings of Hartono et al. (2014), which revealed that confidentiality is essential in forming security. For that reason, the increase in the confidentiality dimension is also predicted to increase perceived security. In this research, the correlation between confidentiality and perceived security was also tested using statistics, and the results showed support for hypothesis 1a with a coefficient of 0.35; $p < 0.01$.

This finding confirms previous studies done by Cegielski (2008), Ryan and Ryan (2007); Turban et al. (2010); Tube et al. (2009). They have agreed that confidentiality would cause a feeling of security in someone to increase. Customers will feel safe when the company provides a guarantee not to reveal their transactions to other parties. If the company's guarantee or recommendation is breached, customers will feel unsafe to transact with the same company.

Hypothesis 1b stated that integrity had a positive correlation with perceived security. This hypothesis is based on Sipponen and Kukkonen's (2007) research, revealing that integrity is essential regarding perceived security. This research also tested the relationship between integrity and perceived security. After conducting statistical tests, the researchers concluded that integrity did not correlate positively with perceived security. It could be seen from the coefficient value of 0.01; $p = 0.25$. The lack of evidence supporting hypothesis 1b was caused by respondents' inability to distinguish between confidentiality and integrity. Even though the results are not as expected, this finding is consistent with Schneider's (2010) and Motro (1992). They revealed that two dimensions: confidentiality and integrity, are closely related. A breach of confidentiality often occurs when a violation of integrity also follows it. Integrity is often equated with confidentiality, despite the two dimensions being different. When an intruder sabotages a message from confidential information, they must first read the information (violating confidentiality) before he can modify that information (breaching integrity). A company may be able to maintain the confidentiality of its customers. However, it is not guaranteed that it maintains integrity. The inability of a company to maintain its integrity will disrupt security. People will easily use other people's identity to execute e-commerce without being discovered by the company. The lack of results supporting this hypothesis has become a signal that there may be a tight relationship between

confidentiality and integrity. At least, the two indicators can be combined as one with the name confidentiality.

Availability refers to the completeness of the information provided to customers. The more the information and the more complete the information available to customers, the higher the security and comfort in transacting (Suh & Han, 2011). Hypothesis 1c stated that there was a positive correlation between availability and perceived security. The higher the availability, the higher the perceived security is expected to be. Hypothesis test results statistically illustrated a positive and significant correlation between the two, with a coefficient value of 0.31; $p < 0.01$. Companies that provide complete information to their customers will always use the companies' websites. They would feel that the company is not concealing any information capable of changing the decision to transact via the website. A company's guarantee to always provide information to its consumers will be followed by a high-security sense to conduct transactions.

Moreover, non-repudiation refers to the assurance that the selling company will not cancel transactions once they are completed. Nearly every study discussing perceived security found a positive and significant correlation with non-repudiation (Bodin et al., 2005). Companies that offer non-repudiation guarantees are predicted to make their customers feel safer when transacting. For that reason, the selling company cannot cancel the transaction once it is completed. Hypothesis 1d stated that non-repudiation correlated positively with perceived security and was statistically supported by the coefficient value of 0.29; $p < 0.01$. This finding strengthens previous findings (Hartono et al., 2014; Turban et al., 2010; Bodin et al., 2005).

Privacy is often misinterpreted as confidentiality, although the two terms are different (Hole, 2008). Furthermore, several studies have also placed privacy and security as two different unrelated things (Turban et al., 2010; Hartono et al., 2014; Suh & Han, 2010). Conversely, Cegielski's (2008) research places the privacy dimension as one of the dimensions forming perceived security. When someone's privacy is disregarded, it will make them feel unsafe when transacting. Hypothesis 1e proposed to strengthen the finding of Cegielski (2008). Statistical analysis results showed that hypothesis 1e was supported by the coefficient value 0.32; $p < 0.01$.

Hypothesis 1f stated that authentication correlated positively with perceived security. Turban et al. (2010) defined authentication as a process to ensure an individual's real identity, computer program, or e-commerce website. It is also related to the identification process before conducting a transaction. Each party must be identified as the buyer (responsible for paying) and the seller (responsible for providing the product and service). Statistical hypothesis test results suggested that hypothesis 1f was not supported by the coefficient value 0.02; p-value = 0.27. This finding is consistent with the findings of Hartono et al. (2014), which revealed that authentication is not one of the dimensions affecting perceived security but rather an attempt to prevent or protect the system from attacks on this security.

Then, perceived security in this study was modeled as a second-order construct measured formatively with five indicators. Subsequently, perceived security was connected to the intention to use B2C websites. Hypothesis 2 stated that perceived security correlated positively to use websites. Statistical hypothesis test results illustrated that hypothesis 2 was supported by the coefficient value 0.25; $p < 0.01$. This result supports the research proposed by Hartono et al. (2014). Companies that provide an optimal security guarantee will increase customers' intention to use their websites to transact. This finding also reinforces perceived risk theory and previous studies (Salisbury, 2001; Lim, 2003; Fang et al., 2006; Cheng et al., 2006). In the e-commerce environment, consumers feel that previous uncertain buying experiences will be one of the causes of potential losses due to a security breach (Casal, Flavian, and Guinalui, 2007). For that reason, customers who feel that a website has a low-security level will also feel that there is a high transaction risk. In exchange, it will decrease their intent to use websites.

Hypothesis 3 stated that perceived security correlated positively with perceived ease of use. Previous studies (Lu et al., 2007) showed a positive correlation between perceived security and perceived ease of use. Statistical hypothesis test results suggested that hypothesis 3 was supported significantly by a coefficient value of 0.64; $p < 0.01$. Perceived ease of use covers individual comfort in using the system (Usoro et al., 2010). The higher the perceived security, the higher the comfort of customers to use it.

Hypothesis 4, stating that perceived security correlates positively with perceived usefulness, was statistically supported by the coefficient value 0.21; $p < 0.01$. There has been no study directly connecting perceived security to perceived usefulness to the researchers' best knowledge. However, a positive correlation between the two seems logical. Gefen, Karahanna, and Straub (2003) expressed that e-commerce applications are divided into short-term and long-term use. An example of long-term use would be a website's ability to prevent or protect its customers from additional costs due to a security breach (use of credit card information by unauthorized parties). It could be concluded that an increase in the perceived security of an e-commerce website would increase consumer confidence, thus providing long-term benefits. It provides support for hypothesis 4.

Further, hypothesis 5 stated that perceived ease of use correlated positively with perceived usefulness. Previous studies (Venkatesh, & Davis, 2000; Davis, 1989) revealed that perceived ease of use directly and significantly impacted perceived usefulness. If a system is easier to use, that system will positively impact its users' performance (greater usefulness). Statistical hypothesis test results indicated that hypothesis 5 was supported significantly by a coefficient value of 0.64; $p < 0.01$. Suppose this hypothesis test result was connected to the use of B2C websites. It would illustrate that easy-to-use websites would provide useful information, thus aids decision making in online transactions.

Furthermore, the hypothesis test results for hypothesis 6 indicated a positive correlation between perceived ease of use and intention to use B2C websites. This statistical test produced a significant coefficient value of 0.17; $p < 0.04$. If this result were connected to

the use of B2C websites, it would illustrate that easy-to-use websites would increase a person's desire to transact online.

Finally, hypothesis 6 stated that perceived usefulness correlated positively to the use of B2C websites. Previous studies (Davis, Bagozzi, & Warshaw, 1989; Venkatesh and Davis, 2000; Salisbury et al., 2001) revealed a positive correlation between the two. However, the data analysis result showed a coefficient value that was no significant (0.05; p = 0.33). This result conflicts with the previously mentioned studies (Davis et al., 1989; Venkatesh and Davis, 2000; Salisbury et al., 2001). However, the insignificant correlation found between these two variables is consistent with the argument that although customers know transacting online is easy and beneficial, they are still reluctant to do so. One of the most plausible explanations is consumers' habit of using traditional transactions (Andersone & Sarkane, 2009). Table 7 shows a summary of the hypothesis test results.

Table 7 Summary of Hypothesis Tests

No.	Hypotheses	Results
1	H1a: Confidentiality correlates positively with perceived security.	Supported
2	H1b: Integrity correlates positively with perceived security.	Not supported
3	H1c: Availability correlates positively with perceived security.	Supported
4	H1d: Non-repudiation correlates positively with perceived security.	Supported
5	H1e: Privacy correlates positively with perceived security.	Supported
6	H1f: Authentication correlates positively with perceived security.	Not supported
7	H2: Perceived security correlates positively with the intention to use B2C e-commerce websites.	Supported
8	H3: Perceived security correlates positively with perceived ease of use.	Supported
9	H4: Perceived security correlates positively with perceived usefulness.	Supported
10	H5: Perceived ease of use correlates positively with perceived usefulness.	Supported
11	H6: Perceived ease of use correlates positively with the intention to use B2C e-commerce websites.	Supported
12	H7: Perceived usefulness correlates positively with the intention to use B2C e-commerce websites.	Not supported

Conclusion

This research is one of the empirical studies conducted to provide evidence on the dimensions of perceived security that increases the intention to use B2C e-commerce websites. Statistical test results support several previous studies revealing that confidentiality, availability, non-repudiation, and privacy are valid dimensions that form perceived security (Cegielski, 2008; Parent, 2007; Gurbani & McGee (2007).

This research aims to test perceived security dimensions with different indicators than previous studies (Hartono et al., 2014; Cegielski, 2008). Inconsistency in the dimensions becomes a gap in which further research is to be conducted. The primary purpose of this

research is to validate the dimensions of perceived security that cover confidentiality, integrity, availability, non-repudiation, privacy, and authentication. Test results in this research revealed that confidentiality, availability, non-repudiation, and privacy were all valid dimensions that form perceived security.

It was evident that the higher a company guaranteed these four dimensions, the higher the perceived security. In this research, the researchers also found no evidence supporting the correlation between integrity and perceived security. However, this is consistent with Schneider's (2010) research and Motro (1992), which revealed that integrity was closely related to confidentiality. A breach of integrity will follow a violation of confidentiality.

This research also revealed that perceived security influenced intention to use B2C e-commerce websites. This finding is consistent with that of Hartono et al. (2014). The higher the perceived security, the higher the customers' intention to use B2C e-commerce websites. Apart from testing the validity of the perceived security, this research also tested the mediating effect of perceived ease of use and perceived usefulness on the relationship between perceived security and intention to use B2C e-commerce websites. Statistical testing uncovered that perceived security had a positive correlation with perceived ease of use and perceived usefulness. This finding is also consistent with previous findings (Salisbury et al., 2001). People who feel safe in transacting will feel comfortable using websites, causing them to use them to transact. However, this study discovered an insignificant correlation between perceived usefulness and intention to use B2C e-commerce websites. This result showed that although a person understood that transacting online was safe and useful, they were still not motivated to use B2C e-commerce websites. This finding is consistent with Andersone and Sarkane (2009), which tested people's preference between an online transaction and a traditional transaction. Andersone and Sarkane (2009) found that although people knew the benefits of transacting online, they would still prefer to transact offline. Other possible explanations for this finding's lack of support include cultural differences between developed and developing countries.

Furthermore, the use of a mandatory system would influence a person's perceived usefulness because although they might feel that the website was of no use to them, they still had to use it as they had been ordered to. This research also supports Hartono et al. (2014) that revealed that authentication is not one of the dimensions forming perceived security. Instead, it attempts to prevent attacks from occurring in a system.

This research is expected to provide two essential contributions to information systems research. Firstly, this research can identify and validate the essential dimensions of perceived security (Hartono, 2014; Shah, Peikari, & Yasin, 2014). Previous studies (Berthon, Pitt, and Campbell, 2008; Chang & Chen, 2009; Peterson, Meinert, Criswell & Crossland, 2007) used the perceived security construct and tended to capture only one dimension or is dominated by only one dimension (for example privacy or non-repudiation). The inclusion of other dimensions (i.e., availability, confidentiality, non-

repudiation, and privacy) reassures that a perceived security construct is consistent with previous studies.

This definition will also promote more detailed analyses of the effects of each dimension of other key variables in the model tested. For example, previous studies have shown that perceived safety has positively affected consumers' intention to use B2C e-commerce websites (Salisbury et al., 2001). Awareness of the validity of perceived honesty, confidentiality, perceived accessibility, and perceived non-repudiation as the dimensions of perceived protection, however, must reveal a more thorough understanding of how the purpose to use component affects buyers' security. Recognizing the key dimensions of perceived security offers researchers an opportunity to add depth to their assessments and highlight each dimension's value to increase the intention to use websites. Secondly, this study contributes to develop and validate the main dimensions of perceived security and their moderating constructs. These multi-dimensional measurements' reliability and validity show that one-dimensional perceived security popular in previous studies is rendered unusable (Hartono, 2014).

Furthermore, this research showed how perceived confidentiality, perceived availability, and perceived non-repudiation are essential dimensions of information system practitioners' perceived security. These dimensions played an essential role in customer decisions on whether to use B2C e-commerce websites. Collectively, these dimensions significantly impacted perceived usefulness, perceived ease of use, trust, and intention to use B2C websites. Compared with previous studies (Ryan & Ryan, 2005; Erlich & Zviran, 2010; Gordon et al., 2011), these dimensions' entrance into the perceived security measurement provides a more comprehensive metric than perceived security. This metric allows managers to develop their understanding to deeper understand the effect of perceived security and customer willingness to use websites for online purchases. This understanding will help them uncover problems related to perceived security and make strategic decisions to improve customer perceived security.

Interpretation of this research results has several limitations. Firstly, this research's empirical results used a sample of Indonesian individuals, which had benefits of limitations on other unwanted factors, such as cultural differences. However, it has also hindered the ability of this research to generalize. Secondly, the use of cross-sectional data caused this research only to be able to test a snapshot of the impacts of various antecedent variables on the actual use of e-commerce websites. Moreover, the third limitation was the use of convenience sampling, which most likely also decreased the ability to generalize results.

Due to time restrictions and budget limitations, future research can be conducted using longitudinal data, which will reveal this phenomenon's dynamics over a much more extensive timeframe. Furthermore, the inclusion of other factors that may affect e-commerce website usages, such as price and trust, can be done in future research.

Appendix

Table A1 Combined loadings and cross-loadings

	CONF	INT	AVA	REPU	PRIV	AUT	SEC	INTUSE	EOU	USE	SE	P-value
CONF 1	**0.863**	-0.509	-0.474	-0.395	-0.428	0.454	-0.209	-0.029	0.157	0.013	0.057	<0.01
CONF 2	**0.867**	0.118	0.11	0.013	0.099	-0.052	-0.183	0.043	-0.164	0.076	0.047	<0.01
CONF 3	**0.861**	0.391	0.364	0.033	0.328	-0.349	0.183	-0.014	0.008	-0.09	0.055	<0.01
INT1	0.161	**0.835**	0.155	0.129	0.14	-0.149	-0.162	-0.034	0.006	0.014	0.046	<0.01
INT2	0.075	**0.896**	0.072	0.065	0.165	-0.169	0.075	0.022	-0.123	0.034	0.037	<0.01
INT3	-0.227	**0.886**	-0.22	-0.183	-0.198	0.21	-0.07	0.009	0.12	-0.047	0.043	<0.01
AVA 1	-0.385	-0.402	**0.848**	-0.313	-0.335	0.356	-0.196	0.093	-0.061	0.102	0.047	<0.01
AVA 2	0.585	0.607	**0.869**	0.471	0.511	-0.54	0.183	0.018	0.098	-0.033	0.037	<0.01
AVA 3	0.313	0.325	**0.88**	0.252	0.273	-0.29	0.171	-0.108	-0.039	-0.066	0.038	<0.01
REPU1	0.118	0.122	0.138	**0.83**	0.102	-0.109	-0.353	-0.052	0.151	-0.062	0.057	<0.01
REPU2	-0.156	-0.162	-0.151	**0.854**	-0.136	0.141	0.142	0.032	-0.02	-0.072	0.055	<0.01
REPU3	0.416	0.432	0.402	**0.864**	0.363	-0.386	0.198	0.018	-0.125	0.131	0.05	<0.01
PRIV1	0.582	0.435	0.625	0.468	**0.875**	-0.538	0.44	-0.028	0.003	-0.04	0.061	<0.01
PRIV2	-0.592	-0.145	-0.572	-0.476	**0.816**	0.548	-0.101	0.008	-0.05	0.012	0.04	<0.01
PRIV3	-0.302	-0.314	-0.292	-0.243	**0.869**	0.025	0.498	0.02	0.045	0.029	0.063	<0.01
AUT1	0.24	0.211	0.197	0.164	0.178	**0.681**	-0.384	0.122	-0.036	0.178	0.112	<0.01
AUT2	-0.405	-0.42	-0.391	-0.326	-0.353	**0.633**	0.4687	-0.149	-0.089	-0.084	0.118	<0.01
AUT3	0.156	0.162	0.151	0.126	0.136	**0.552**	-0.477	0.151	0.108	-0.09	0.101	<0.01
lv_CONF	0.104	0	0.004	0.004	0.004	0	**0.842**	0	0	0	0.054	<0.01
lv_AVA	-0.028	0	0.974	-0.025	-0.026	0	**0.776**	0	0	0	0.053	<0.01
lv_REPU	-0.133	0	-0.123	0.882	-0.123	0	**0.743**	0	0	0	0.068	<0.01
lv_PRIV	-0.135	0	-0.862	-0.825	0.139	0	**0.775**	0	0	0	0.064	<0.01
INTUSE1	0.346	0.196	0.475	0.454	0.474	-0.154	0.431	**0.669**	0.328	-0.154	0.087	<0.01
INTUSE2	-0.177	-0.211	-0.163	-0.156	-0.1633	0.216	0.0519	0.713	-0.175	0.204	0.098	<0.01
INTUSE3	-0.281	0.025	-0.259	-0.248	-0.2591	-0.066	0.082	0.776	-0.123	-0.055	0.071	<0.01
EOU1	-0.089	-0.075	-0.51	-0.488	-0.051	-0.008	0.162	-0.06	0.861	-0.065	0.055	<0.01
EOU2	0.379	0.194	0.157	0.314	0.1567	0.082	-0.498	-0.041	0.872	-0.005	0.043	<0.01
EOU3	-0.325	-0.158	-0.135	-0.133	-0.139	0.095	0.441	0.130	0.667	0.09	0.113	<0.01
USE1	0.342	0.164	-0.09	-0.087	-0.090	0.086	0.288	-0.008	0.072	0.855	0.065	<0.01
USE2	0.582	0.024	0.189	0.181	0.189	0.084	-0.06	-0.024	-0.061	0.841	0.049	<0.01
USE3	-0.097	-0.18	-0.193	-0.88	-0.0918	0.089	0.291	0.03	-0.011	0.888	0.072	<0.01

Table A2 Indicator Weight

	CONF	INT	AVA	REPU	PRIV	SECURIT	INTUSE	SE	P-value	VIF
CONF 1	0.386	0	0	0	0	0	0	0.024	<0.01	1.892
CONF 2	0.388	0	0	0	0	0	0	0.028	<0.01	1.93
CONF 3	0.385	0	0	0	0	0	0	0.023	<0.01	1.876
INT1	0	0.365	0	0	0	0	0	0.021	<0.01	1.73
INT2	0	0.392	0	0	0	0	0	0.018	<0.01	2.348
INT3	0	0.388	0	0	0	0	0	0.019	<0.01	2.247
AVA 1	0	0	0.377	0	0	0	0	0.019	<0.01	1.794
AVA 2	0	0	0.386	0	0	0	0	0.02	<0.01	1.976
AVA 3	0	0	0.391	0	0	0	0	0.02	<0.01	2.068
REPU1	0	0	0	0.383	0	0	0	0.028	<0.01	1.644
REPU2	0	0	0	0.394	0	0	0	0.027	<0.01	1.792
REPU3	0	0	0	0.399	0	0	0	0.024	<0.01	1.862
PRIV1	0	0	0	0	0.4	0	0	0.019	<0.01	2.004
PRIV2	0	0	0	0	0.373	0	0	0.035	<0.01	1.590
PRIV3	0	0	0	0	0.397	0	0	0.022	<0.01	1.955
lv_CONF	0	0	0	0	0	0.368	0	0.016	<0.01	**2.244**
lv_INT	0	0	0	0	0	0.378	0	0.02	<0.01	**2.026**
lv_AVA	0	0	0	0	0	0.398	0	0.018	<0.01	**2.289**
lv_REPU	0	0	0	0	0	0.376	0	0.02	<0.01	**1.452**
lv_PRIV	0	0	0	0	0	0.335	0	0.021	<0.01	**1.593**
INTUSE1	0	0	0	0	0	0	0.429	0.055	<0.01	1.108
INTUSE2	0	0	0	0	0	0	0.458	0.065	<0.01	1.143
INTUSE3	0	0	0	0	0	0	0.498	0.048	<0.01	1.195

References

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: a review and recommended two-step approach. *Psychological Bulletin, 103*(3), 411-423. https://doi.org/10.1037/0033-2909.103.3.411

Andersone and E Gaile-Sarkane. (2009). Impact of technology adoption on customer behavior. Ekonomika IR, Vadyba. 14. ISSN 1822-6515.

Azizi, S., & Javidani, M. (2010). Measuring e-shopping intention: An Iranian perspective. *African Journal of Business Management, 4*(13), 2668–2675. Retrieved from https://academicjournals.org/journal/AJBM/article-full-text-pdf/FD5EB9523796

Bagozzi, R.P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science 16*. 74–94. https://doi.org/10.1007/BF02723327

Balapour, A., Nikkhah, H. R., & Sabherwal, R. (2020). Mobile application security: Role of perceived privacy as the predictor of security perceptions. *International Journal of Information Management, 52*, 102063. https://doi.org/10.1016/j.ijinfomgt.2019.102063

Belanger, F., Hiller, J.S., & Smith, W.J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The Journal of Strategic Information Systems*, *11*(3–4): 245–270. https://doi.org/10.1016/S0963-8687(02)00018-5

Bella, G., Giustolisi, R., & Riccobene, S. (2011). Enforcing privacy in e-commerce by balancing anonymity and trust. *Computers & Security, 30*(8), 705–718. https://doi.org/10.1016/j.cose.2011.08.005

Berthon, P., Pitt, L., & Campbell, C. (2008). Ad Lib: When customers create the ad. *California Management Review, 50*(4), 6-30. Retrieved from https://research.monash.edu/en/publications/ad-lib-when-customers-create-the-ad

Bhatnagar, A., Misra, S., & Rao, H. R. (2000). On risk, convenience, and Internet shopping behavior. *Communications of the ACM, 43*(11), 98–105. https://doi.org/10.1145/353360.353371

Bodin, L. D., Gordon, L. A., & Loeb, M. P. (2005). Evaluating information security investments using the analytic hierarchy process. *Communications of the ACM, 48*(2), 78–83. https://doi.org/10.1145/1042091.1042094

Cegielski, C. G. (2008). Toward the development of an interdisciplinary information assurance curriculum: knowledge domains and skill sets required of information assurance professionals. *Decision Sciences Journal of Innovative Education, 6*(1), 29–49. https://doi.org/10.1111/j.1540-4609.2007.00156.x

Chang, H. H., & Chen, S. W. (2009). Consumer perception of interface quality, security, and loyalty in electronic commerce. *Information & Management, 46*(7), 411–417. https://doi.org/10.1016/j.im.2009.08.002

Chellappa, R. K., & Pavlou, P. A. (2002). Perceived information security, financial liability, and consumer trust in electronic commerce transactions. *Logistics Information Management, 15*(5/6), 358–368. https://doi.org/10.1108/09576050210447046

Cheng, T. C. E., Lam, D. Y. C., & Yeung, A. C. L. (2006). Adoption of internet banking: An empirical study in Hong Kong. *Decision Support Systems, 42*(3), 1558–1572. https://doi.org/10.1016/j.dss.2006.01.002

Cheung, C. M., & Lee, M. K. (2001). Trust in internet shopping: instrument development and validation through classical and modern approaches. *Journal of Global Information Management 9*(3). 23–35. https://doi.org/10.4018/jgim.2001070103

Clarke, R. (1998). *Message transmission security*. Retrieved from Xamax Consultancy Pty Ltd. Available at http://www.rogerclarke.com/II/CryptoSecy.html

Cooper, D. R., & Schindler, P. S. (2006). *Business Research Methods. 9 Edition*. New York: McGraw-Hill.

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika, 16*(3), 297–334. https://doi.org/10.1007/bf02310555

Crosby, L. A., Evans, K. R., & Cowles, D. (1990). Relationship quality in services selling: an interpersonal influence perspective. *Journal of Marketing, 54*(3), 68–81. https://doi.org/10.1177/002224299005400306

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-340. https://doi.org/10.2307/249008

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management Science, 35*(8), 982–1003. https://doi.org/10.1287/mnsc.35.8.982

Diamantopoulos, A., & Winklhofer, H. M. (2001). Index construction with formative indicators: An alternative to scale development. *Journal of Marketing Research, 38*(2), 269–277. https://doi.org/10.1509/jmkr.38.2.269.18845

Diamantopoulos, A., Riefler, P., & Roth, K. P. (2008). Advancing formative measurement models. *Journal of Business Research, 61*(12), 1203–1218. https://doi.org/10.1016/j.jbusres.2008.01.009

Erlich, Z., & Zviran, M. (2010). Goals and practices in maintaining information systems security. *International Journal of Information Security and Privacy, 4*(3), 40–50. https://doi.org/10.4018/jisp.2010070103

Fang, Y., Qureshi, I., Sun, H., McCole, P., Ramsey, E., & Lim, K. (2014). Trust, satisfaction, and online repurchase intention: the moderating role of perceived effectiveness of e-commerce institutional mechanisms. *MIS Quarterly, 38*(2), 407-428(A9). https://doi.org/10.25300/misq/2014/38.2.04

Flavián, C., & Guinalíu, M. (2006). Consumer trust perceived security and privacy policy: three basic elements of loyalty to a website. *Industrial Management & Data Systems, 106*(5), 601–620. https://doi.org/10.1108/02635570610666403

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50. https://doi.org/10.1177/002224378101800104

Gefen, D. (2000). E-commerce: the role of familiarity and trust. *Omega, 28*(6), 725–737. https://doi.org/10.1016/s0305-0483(00)00021-9

Gefen, D., Karahanna, E., & Straub, D. (2003). Trust and tam in online shopping: An integrated model. *MIS Quarterly, 27*(1), 51-90. https://doi.org/10.2307/30036519

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security, 19*(1), 33–56. https://doi.org/10.3233/jcs-2009-0398

Grazioli, S., & Jarvenpaa, S. L. (2000). Perils of Internet fraud: an empirical investigation of deception and trust with experienced Internet consumers. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 30*(4), 395–410. https://doi.org/10.1109/3468.852434

Gurbani, V. K., & McGee, A. R. (2007). An early application of the bell labs security framework to analyze vulnerabilities in the internet telephony domain. *Bell Labs Technical Journal, 12*(3), 7–19. https://doi.org/10.1002/bltj.20246

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate Data Analysis. Seventh Edition*. New Jersey: Prentice-Hall.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2006). *Multivariate data analysis (6th ed.)*. Upper Saddle River, NJ: Pearson University Press.

Hartono, E., Holsapple, C. W., Kim, K.-Y., Na, K.-S., & Simpson, J. T. (2014). Measuring perceived security in B2C electronic commerce website usage: A respecification and

validation. *Decision Support Systems, 62*, 11–21. https://doi.org/10.1016/j.dss.2014.02.006

Hartono. (2008). *SPSS. 16.0. Analisa Data Statistika dan Penelitian.* Yogyakarta: Pustaka Pelajar.

Hole, K.J. Tjøstheim, T., Moen, V., Netland, L., Espelid, Y., & Klingsheim, A.N. (2007). Next-generation internet banking in Norway. Retrieved from IEEE Security & Privacy. Available at http://www.nowires.org/Papers-PDF/BankIDevaluation.pdf

Hootsuite (2020). Retrieved from We Are Social. Available at https://datareportal.com/reports/digital-2020-indonesia

Jarvis, C. B., MacKenzie, S. B., & Podsakoff, P. M. (2003). A critical review of construct indicators and measurement model misspecification in marketing and consumer research. *Journal of Consumer Research, 30*(2), 199–218. https://doi.org/10.1086/376806

Keil, M., Lee, H.K., & Deng, T. (2013). Understanding the most critical skills for managing I.T. projects: a Delphi study of I.T. project managers. *Information Management 50*(7) 398–414. https://doi.org/10.1016/j.im.2013.05.005

Kiang, M. Y., Ye, Q., Hao, Y., Chen, M., & Li, Y. (2011). A service-oriented analysis of online product classification methods. *Decision Support Systems, 52*(1), 28–39. https://doi.org/10.1016/j.dss.2011.05.001

Kim, C., Tao, W., Shin, N., & Kim, K.-S. (2010). An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic Commerce Research and Applications, 9*(1), 84–95. https://doi.org/10.1016/j.elerap.2009.04.014

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems, 44*(2), 544–564. https://doi.org/10.1016/j.dss.2007.07.001

Kurt, G., & Hacioglu, G. (2010). Ethics as a customer perceived value driver in the context of online retailing. *African Journal of Business Management, 4*(5), 672-677. https://doi.org/10.5897/AJBM.9000265

Laudon, K. C., & Traver, C.C. (2019). *E-Commerce 2019: Business. Technology. Society. Fifteenth Edition.* Hoboken: Pearson

Lian, J., & Lin, T. (2008). Effects of consumer characteristics on their acceptance of online shopping: Comparisons among different product types. *Computers in Human Behavior,* 48–65. https://doi.org/10.1016/j.chb.2007.01.002

Lim, N. (2003). Consumers' perceived risk: sources versus consequences. *Electronic Commerce Research and Applications, 2*(3), 216–228. https://doi.org/10.1016/s1567-4223(03)00025-5

Lu, C.-S., Lai, K., & Cheng, T. C. E. (2007). Application of structural equation modeling to evaluate the intention of shippers to use Internet services in liner shipping. *European Journal of Operational Research, 180*(2), 845–867. https://doi.org/10.1016/j.ejor.2006.05.001

Matic, M., & Vojvodic, K. (2014). customer-perceived insecurity of online shopping environment. *International Review of Management and Marketing, 4*(1), 59-65. Retrieved from https://econjournals.com/index.php/irmm/article/view/677

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *The Academy of Management Review, 20*(3), 709–734. https://doi.org/10.2307/258792

McKnight, D. H., & Chervany, N. L. (2001). What trust means in e-commerce customer relationships: an interdisciplinary conceptual typology. *International Journal of Electronic Commerce, 6*(2), 35–59. https://doi.org/10.1080/10864415.2001.11044235

Mitchell, V.L. (2006). Knowledge integration and information technology project performance. *MIS Quarterly 30*(4), 919–939. https://doi.org/10.2307/25148759

Motro, A. (1992). A unified model for security and integrity in relational databases. *Journal of Computer Security, 1*(2), 189–213. https://doi.org/10.3233/jcs-1992-1204

Oni, O.O., & Adeyeye, M.M. (2020). Digital commerce security and customer satisfaction in southwest Nigeria. *Fountain University Osogbo Journal of Management 5*(2), 69-81. Retrieved from http://www.osogbojournalofmanagement.com/index.php/ojm/article/view/160

Parent, M. (2007). The 6th and biggest lie of all: Lessons from a decade of e-tailing. *Ivey Business Journal 71*(8) 1-7. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=27982288&site=ehost-live

Peterson, D., Meinert, D., Criswell, J., & Crossland, M. (2007). Consumer trust: privacy policies and third party seals. *Journal of Small Business and Enterprise Development, 14*(4), 654-669. https://doi.org/10.1108/14626000710832758

Podsakoff, P. M., & Organ, D. W. (1986). Self-reports in organizational research: problems and prospects. *Journal of Management, 12*(4), 531–544. https://doi.org/10.1177/014920638601200408

Ransbotham, S., Mitra, S., & Ramsey, J. (2012). Are markets for vulnerabilities effective? *MIS Quarterly, 36*(1), 43-64. https://doi.org/10.2307/41410405

Roca, J. C., García, J.J., & de la Vega, J.J. (2009). The importance of perceived trust, security, and privacy in online trading systems. *Information Management & Computer Security, 17*(2), 96–113. https://doi.org/10.1108/09685220910963983

Ryan, J. J. C. H., & Ryan, D. J. (2005). Proportional hazards in information security. *Risk Analysis, 25*(1), 141–149. https://doi.org/10.1111/j.0272-4332.2005.00573.x

Salisbury, W., Pearson, R., Pearson, A.W., & Miller, D. (2001). Perceived security and worldwide web purchase intention. *Industrial Management & Data Systems, 101*(4), 165–177. https://doi.org/10.1108/02635570110390071

Schneider, G.P. (2010). *Electronic commerce, 9th ed.* Cengage Learning.

Shah, M. H., Peikari, H. R., & Yasin, N. M. (2014). The determinants of individuals' perceived e-security: Evidence from Malaysia. *International Journal of Information Management, 34*(1), 48–57. https://doi.org/10.1016/j.ijinfomgt.2013.10.001

Sholihin, M. & Ratmono, D. (2013). *Analisis SEM-PLS dengan WarpPLS 3.0 untuk hubungan nonlinier dalam penelitian sosial dan bisnis*. Yogyakarta: Andi Offset.

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 38*(1), 60–80. https://doi.org/10.1145/1216218.1216224

Statista. (2019). E-commerce in Indonesia. Retrieved from Statista. Available at https://www.statista.com/study/60342/e-commerce-in-indonesia/

Suh, B., & Han, I. (2002). Effect of trust on customer acceptance of Internet banking. *Electronic Commerce Research and Applications, 1*(3-4), 247–263. https://doi.org/10.1016/s1567-4223(02)00017-0

Tsiakis, T., & Sthephanides, G. (2005). The concept of security and trust in electronic payments. *Computers & Security, 24*(1), 10–15. https://doi.org/10.1016/j.cose.2004.11.001

Turban, E., King, D., Lee, J. K., Liang, T.-P., & Turban, D. C. (2010). *Electronic Commerce. A Managerial Perspective Global Edition*. New Jersey: Pearson.

Usoro, A., Shoyelu, S., & Kuofie, M. (2010). Task-technology fit and technology acceptance models applicability to e-tourism. *Journal of Economic Development, Management, I.T.,*

Finance and Marketing, 2(1), 1–32. Retrieved from https://research-portal.uws.ac.uk/en/publications/task-technology-fit-and-technology-acceptance-models-applicabilit

Vaidyanathan, G., & Mautone, S. (2009). Security in dynamic web content management systems applications. *Communications of the ACM, 52*(12), 121–125. https://doi.org/10.1145/1610252.1610284

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: four longitudinal field studies. *Management Science, 46*(2), 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926

Yousafzai, S., Pallister, J., & Foxall, G. (2009). Multi-dimensional role of trust in Internet banking adoption. The Service Industries Journal, 29(5), 591–605. https://doi.org/10.1080/02642060902719958