INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 14, Issue 8, (2024) E-ISSN: 2222-6990

The Cryptography Technology Usage in Message System: Online Shoppers Perspective

Azrina Othman[1], Norhidayah Mohamad[1], Nik Adzrieman Abdul Rahman[2], Adilah Mohd Din[1]

[1]Faculty of Technology Management and Technopreneurship, Universiti Teknikal Malaysia Melaka, Jalan Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia, [2]Faculty of Multimedia Technology and Communication, Universiti Utara Malaysia, Sintok, 06010 Bukit Kayu Hitam, Kedah,Malaysia

Email: azrina@utem.edu.my

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v14-i8/22586 DOI:10.6007/IJARBSS/v14-i8/22586

Published Date: 30 August 2024

Abstract

This research explores the essential role of cryptography in securing messaging systems within online shopping platforms, with a focus on consumer perspectives in Malaysia. As online shopping becomes increasingly prevalent, the need for secure communication to protect sensitive information and maintain consumer trust is paramount. The study utilizes the Technology Acceptance Model (TAM) to examine factors influencing the adoption of cryptography technology among online shoppers. A survey of 150 Shopee users was conducted to gather insights on their perceptions of the technology's usefulness, ease of use, confidentiality, and non-repudiation. Data analysis using SPSS, including descriptive statistics, Pearson correlation, and linear regression, revealed that all four factors significantly impact the adoption of cryptography, with non-repudiation being the most influential. The findings suggest that consumers prioritize the assurance that their messages cannot be altered or denied, underscoring the need for strong cryptographic protections in online shopping platforms. However, the study faced limitations due to the COVID-19 pandemic, which restricted data collection to online methods. Future research should broaden the scope by including a more diverse demographic and geographical representation and incorporating in-depth interviews with industry experts. These steps would provide further insights into the effectiveness of different cryptographic methods across various platforms and industries.

Keywords: Online Shopping, Message System, Cryptography, Security, Consumer Trust.

Introduction

Online shopping has become a multi-billion-dollar business in the last several decades. Online shopping has become an ordinary activity for millions of individuals worldwide. In recent times, there has been a growth in the number of individuals buying products and services online. The experience that companies can provide their customers is one of the reasons why

online shopping has increased so significantly over the years. In order to offer companies, the same assistance and comfort as they would during the individual purchasing experience, we see companies adding new features and new service to online customers. (Maryam Mohsin, 2020)

First, shoppers began shifting from brick and mortar to websites. Now, they went from desktop shopping to mobile shopping. Shoppers utilise their mobile devices for researching products, comparing their costs, reading product reviews and shopping. In fact, 62% of smartphone users had purchased products online within the previous six months on mobile devices. Mobile shopping was expected to double in 2016 by 34% of all online shopping worldwide, as of the end of 2017. It is only logical, therefore, to try to contact customers using the same gadgets they acquire on online shopping platforms. So, the new mode of communication between the sellers and shoppers are message system. Texts and in-app messages used for the communication between sellers and the shoppers, advertisements, and even for providing suggestions and recommendations online. (Alexa Lemzy, 2018) The threats to security of online shopping caused chaos. Annual successful threats are up to 32.4 per cent for the industry. Hackers generally target administrators, shoppers and employees of online shopping platforms using many harmful tactics. (Jinson Varghese, 2021) In an online shopping platform that causes frauds, many customers reveal their original names, identification card numbers, telephone number and other personal information. Use of the online shopping platform is not usually checked by the customers and information freely shared. Cryptography technology may be utilised as one of the solutions to resolve this problem.

Cryptography is a technology which helps to protect information by converting it into a form which unintended users cannot comprehend. The cryptographic communication, which can be read from an original human, is called plaintext, is transformed to something which an untrained observer would appear like gibberish by means of an algorithm or a sequence of mathematical operations and this gibberish is called ciphertext. Encryption is a technique through which plaintext is turned into ciphertext. Encryption is a key element of cryptography technology, although it does not cover the whole of science. The opposite of encryption is decryption which is a method that converts encrypted data into their original form. Encryption and decryption are the two functions in cryptography technology. (Josh Fruhlinger, 2020)

To achieve the aims of this study, the following research objectives have been established:
1. To define and describe the secure messaging system used in online shopping platforms.
2. To examine the factors through which cryptography protects messaging systems on online shopping platforms.
3. To determine the relationship between cryptography technology and messaging systems within online shopping platforms.

The Application of Cryptography in Message System Among Online Shoppers

Technology is one of the most confusing buzzwords in our society. It appears vital as an analytical category for our comprehension of and indeed beyond the history of all humankind. The term 'technology' has its origins in Indo-European root ‘tek,' which was presumably used to refer to the construction by wattling of wooden buildings, that is, the weaving of sticks. Tek is the Greek technology, which first developed abilities in wood making and quickly became

specialised experts, knows "how" which refers to how things that otherwise would not exist may be made.

Cryptography is a technology of safeguarding information and communication by use of codes, so that the information is read and processed by those for whom it is meant. (Kathleen, 2020) The word cryptography technology comes from the Greek words kryptos which mean "hidden" and grafein which means "to write." During the history of cryptography technology, communications that may otherwise be intercepted were employed for hiding within traditional channels of communication. This is done through disclosure of the content of the communication to everyone other than those who have the key to disclosure. Modern cryptography technology uses e-mail, internet-borne information, credit card information and company network data to safeguard messages. (Charles Edge & Daniel O'Donnell, 2016)

The message system is a component of the telephone, online or mobile communication services which produces text or instant messaging service. It employs defined communication protocols for the exchange of short text messages via fixed line and mobile telephone devices. Messaging is the responsibility of the message system to convey data to another application so that the applications may focus on the data they need to exchange rather than how to transmit it. This mechanism is not safe, however, during transfers from sender to receiver, anybody may access or change the message. (Rahman, 2016) Message system is a safe communication system that allow people to exchange short text messages through online or mobile communication services, which tends to make a messaging service for an online shopping platform.

It may be known as a secure message where any Internet user globally may carry out secret and authenticated exchanges when messaging is constructed with cryptographically constructed methods. Secure messages do not refute the receivers, as the interactions documented via the secure messaging network are individually recognised. Secure communications are usually stored on a physically secure network or internet server, and they are encrypted when data is received or transmitted. The electronic message transfer across a software network immediately shows the message securely in a window on the recipient's screen. (Rahman, 2016) For instance, if a consumer sends a message to a seller in Shopee about purchasing a product, and Shopee implements a cryptographic system on its site, then the message will be secured between the customer and seller only.

Importance of Cryptography

Cryptography technology encrypts the message and decrypts the message from the recipient's side before transmitting it. In this way, even if it is intercepted while delivering a message across the network, it is unreadable. This method allows users to transmit encrypted communications via chats, to encrypt or to decrypt communications without sending them. A hidden message is encoded in the chip text using an appropriate cryptography technology type via random placement. This procedure is quite useful and strong. It helps to confirm that a secret key is valid by comparing it to the genuine secret key of the message when it is extracted from the chip where the key is inserted. (Ghazy Assassa et al, 2009).

Many in online exchange their privacy and secrets. Whether or not they like it, their digital imprint is online. Specifically, anything they say is generally unencrypted and accessible to manipulation by cyber criminals. Cryptography is to identify techniques of protecting sensitive or secret information is therefore urgently required. The key for internet security lies on effective encryption and decoding of data. In this way, information has to be converted to an unreadable format so that only those permitted to do so may be secured and accessed. (Muharrem Tuncay, 2019)

Factors That Cryptography Has to Protect The Message System in The Online Shopping Platform

Besides that, this model is an expansion of the Theory of Reasoned Action (TRA) and Theory of Planned Behaviour (TPM) by Fishbein and Ajzen in 1975. Consequently, two significant believes formed the TAM. (Jose Carlos et al, 2017) The TAM model simultaneously defines the intention of potential use to embrace a new technology in the perceived usefulness (PU) and perceived ease of use (PEOU).

Furthermore, Davis defines perceived usefulness as "the degree to which an individual believed that a system would improve his or her work performance". In the case of cryptography technology, it might be viewed to be advantageous in fields such as online shopping. (Nicole Jonker, 2019) If customers think that the system is beneficial for success, they are more inclined to deploy it faster in the business. (Redzuan et al, 2016) A system with a highly perceived usefulness feels that a user has a positive association between uses and performances. Perceived ease of use defined as "the degree to which a person thought it would be easy to utilise a specific system." by Davis. (Nicole Jonker, 2019) The use of cryptography technology should not involve excessive customer effort. The technology should, for example, be clear to grasp from the start. The message system, on which the cryptography technology operates, is a well disseminated and used technology also has to be noticed.

In addition, according to TAM, perceived usefulness (PU) and perceived ease of use (PEU) have an effect on the attitude towards system use that affect the behavioral intention to use a system that, in turn, defines the actual use of the system. The model is highly important for the study as it provides the basis for building the cryptography technology model. It is a theory that the study theoretically fills the gap between cryptography technology transmissions in a safe manner. (Laszlo Reynolds & Johnson Winks, 2021).

Method Participants

The researcher determines the sample size using the sample-to-item ratio, as outlined by Mumtaz Ali Memon et al. (2020). This method dictates that the ratio should be no less than 5-to-1, meaning that for every item or question in the study, there should be at least five respondents. For example, to study 24 items or questions, a minimum of 150 respondents is required. Consequently, the survey will be conducted among 150 online shoppers across Peninsular Malaysia, focusing on individuals who have used messaging systems within online shopping platforms. These respondents have been specifically selected based on their experience with both online shopping and the messaging systems in question. The selection of appropriate sampling design is crucial for identifying the population and sample necessary

for the research. Therefore, purposive sampling was employed to target online shoppers in Peninsular Malaysia for participation in the study.

Procedure and Measures

The researchers employ a data collection questionnaire as their primary research strategy to obtain quantitative insights from a sample population, which will then be analyzed, evaluated, and summarized. The questionnaire was a structured into three distinct sections: the first will gather demographic information about online shoppers, the second will focus on dependent variables related to messaging systems, and the third will address independent variables concerning cryptography. To capture detailed attitudes and opinions, a 5-point Likert scale will be used, ranging from (1) strongly disagree to (5) strongly agree. This scale allows for more nuanced responses than simple yes/no questions, providing a better understanding of respondents' views on the subject. The questionnaire was distributed to 150 online shoppers across Peninsular Malaysia via Google Forms. To ensure the accuracy and reliability of the data collected, the researchers will conduct a pilot test with 30 respondents. This pilot testing was evaluated the validity and reliability of the instrument, focusing on aspects such as cryptography, perceived usefulness, and ease of use. Despite using established tools from peer-reviewed sources, this piloting process is crucial for confirming the questionnaire's effectiveness and ensuring that it captures meaningful and reliable data before full-scale distribution.

Data Analysis

The popular statistical software packages, such as SPSS (Statistical Package for the Social Sciences), often default to analyzing simple random samples. However, specialized modules or procedures are available for analyzing complex sample data, such as those provided by SPSS (Danjie Zou et al., 2020). The researcher use SPSS version 26 to conduct statistical analysis, manipulate, and summarize the data. SPSS, a commercially distributed software suite developed and marketed by IBM, offers versions for Windows, Mac, and Linux, with major upgrades released approximately every two years (Felix Frey, 2017). The software includes tools for creating charts and graphs, along with standard statistical methods. The analysis involves three main tools: descriptive analysis, pearson correlation, and linear regression analysis.

Descriptive Analysis involves creating basic frequency distributions and summarizing data into single statistics that represent the entire dataset. Descriptive statistics, including measures of central tendency like the mean, median, and mode, offer a summary of the data's key features (Ray Cooksey, 2020).

Pearson Correlation Analysis is used for data that follows a bivariate normal distribution, measuring the strength and direction of a linear relationship between two variables. The Pearson correlation coefficient ranges from –1 to +1, with 0 indicating no correlation and values approaching ±1 indicating a stronger linear relationship (Schober et al., 2018). This analysis assesses the relationship between cryptography and messaging systems in online platforms.

Linear Regression Analysis is based on statistical principles such as sampling, probability, and hypothesis testing (Chuda Dhakal, 2018). This method used to determine how independent variables such as perceived usefulness, perceived ease of use, confidentiality, and non-repudiation that affect the dependent variable of secure messaging systems in online shopping platforms. The researcher will use regression analysis in SPSS version 26 to evaluate these effects.

Results and Discussion

The first component, Section A, has questions about 'Age', 'Gender', 'Employment Status', 'In which state do the respondents live', and 'Can secure message system in online shopping platform described as an internet or mobile communication service that allows customers to send short text messages in a safe and secure manner'. Followed by Section B, a dependent variable that focuses on 'Securing message system among online shoppers.' Furthermore, Section C as the last section, which was an independent variable that consists of the 'Factors that cryptography technology usage has to protect the message system in the online shopping platform' have been discussed.

Demographic analysis is to find out who uses the messaging systems in online shopping platform. There were 150 respondents who completed the questionnaires and their basic demographic information was analysed. As shown in table 1, the highest customer using this application was aged between 19-29 years old. According to Aaron Smith and Monica Anderson in 2016, when it comes to making purchases online, over 90% of young adults between the ages of 18 and 29 have done so because the use of smartphones and social media platforms to participate in commercial activity is highly common among teenagers in particular. Individuals from this age group has the power to negotiate, willing to spend more time and money in online buying and extremely active in online activities. According to Kasasa in 2021, individuals aged from 19- 29 years old are from the Gen Y and Gen Z. Those from Gen Y and Gen Z shop online at a higher rate than individuals from older generations. Web-enabled gadgets are used by individuals from this generation in practically every area of their lives, even when shopping in physical locations. The ease of omnichannel accessibility throughout their shopping trip is demanded by 68 percent of Generation Y and Generation Z, which implies having an integrated experience that can seamlessly convert their consumer data from a smartphone, to a laptop, to a local store, and back again.

This proved the reason why the researchers choose the respondents from this age groups. Furthermore, most of the online shoppers were the female based on this research. According to Dasha M (2019), in general, a significantly higher proportion of females than males choose to purchase online which represents 72% of female, 68% male. The explanation for this is that females love the buying experience as a whole and tend to spend more time shopping online than males. It explained why the majority of my respondents was female. Besides that, the "Others in this question refers to people from the LGBTQ community because they also play important part in online shopping. Moreover, when compare to other employment status, students had the highest frequency which was 101 out of 150.

Table 1
Respondent Profile

Demographic	Dropdown	Frequency	Percent (%)
	18 years old and below 19-29 years old	6	4.0
	30-39 years old	131	87.3
Age	40-49 years	2	1.3
	50 years old and above	5	3.3
		6	4.0
	Male Female	30	20.0
Gender	Others	119	79.3
		1	0.7
	Student Working	101	67.3
	Housewife/Househusband Retired	40	26.7
Employment Status	Others	4	2.7
		1	0.7
		4	2.7
	Perlis Kedah Kelantan Terengganu	4	2.7
	Pahang	8	5.3
	Pulau Pinang Melaka	10	6.7
In which state do you live?	Negeri Sembilan Perak	5	3.3
	Selangor Kuala Lumpur Johor	9	6.0
		5	3.3
		11	7.3
		7	4.7
		6	4.0
		58	38.7
		10	6.7
		17	11.3
Can secure message system in online shopping platform described as an internet or mobile communication service that allows customers to send short text messages in a safe and secure manner?	Yes No	146	97.3
		4	2.7

According to Heri Kuswanto (2019), the Association of Internet Service Providers (APJII) showed that 89.7% of students engaged in online shopping, placing them as the top users in terms of proportion of the total population of internet users. This was due to the fact that a student's desire to engage in online shopping heavily influenced by his or her social circle and surrounding environment. They are most likely to be affected by external variables such as friends and individuals in their circle. On the other hand, 'Others' refers to other categories such as unemployed, blacklisted people, and waiting for jobs. The researcher included the 'Others' category because even individuals in that category shops online regularly. Apart from that, most online customers were from the state of Selangor. According to the Department of Statistics Malaysia (DOSM), the state of Selangor has the highest proportion of customers on online shopping platforms in 2019. The numbers, according to the agency, were gathered through a survey performed in 2019 among eight million households across the country. Based on the statistics, 2.22 million households in Selangor spent money on online shopping platforms over the span of the last several years. That was reason why most of my respondents are from Selangor.

There has never been a greater demand for online shopping. Online shopping had become more popular as a result of the growth of e-commerce and the resulting demand from customers for it. Online shopping is growing more diversified. Online shopping has become immensely simple and convenient in part because of the rapid advancement of technology. The online storefront also provides a broader variety than a single storefront, allowing customers to access products and services that may not be accessible in a local physical shop. Furthermore, as a result of the epidemic, everything had been moved online in order to prevent people from coming into touch with one another. The majority of consumers had begun to utilise an online shopping platform. The purpose of this study was to determine the usage of cryptography technology in message system among female online shoppers. Perceived usefulness (PU), Perceived Ease of Use, Confidentiality and Non-Repudiation, the independent variables derived from prior research, was used to identify a secure message system in order to find the solution to the research problem that was described in this study.
Objective 1: To understand the role of the secure message system in online shopping platform.
Objective 2: To study the factors of cryptography technology usage that effect the message system in the online shopping platform.

Objective 3: To identify the relationship between the usage of cryptography technology and message system in online shopping platform.
In order to study the relationship between the independent and dependent variables, a hypothesis was also developed. On the basis of the hypothesis, the relationship between perceived usefulness (PU), perceived ease of use (PEOU), confidentiality (C), and non-repudiation (NR) with securing message system among female online shoppers(S). In this part, the hypothesis was tested in order to analyse the connection between the independent and dependent variables in order to meet the research goals in this study. As a result, the outcomes were examined in order to determine whether or not the study was successful in achieving the goal.

The questionnaire data was utilised to determine the first objective, which was achieved by using the descriptive statistics. Data are often averaged to determine central tendency (NCSS Statistic, 2016; Manikandan, 2015). Therefore, the nominal scale which was ‘Can secure message system in online shopping platform described as an internet or mobile communication service that allows female online shoppers to send short text messages in a safe and secure manner’, with answers of Yes or No as the answers to the question that the consumer replied.
The result of the descriptive statistics that showed on Table 2 was the description of the secure message system in online shopping platform. By answering 'Yes', 146 respondents (97.3%) agreed that secure message system plays a role as an internet or mobile communication services that lets female online shoppers send short text messages over an online shopping platform in a way that is safe and private. According to Jack Chen et al (2014), a secure message system is a method of encrypting and protecting sensitive information. In this case, the data protected using a server-based solution that prevents data from being shared to others in violation of rules and regulations. A secure message system for female online shoppers is a type of internet or mobile communication service that allows female online shoppers to exchange brief text messages in a protected way.

Table 2
The role of the secure message system in online shopping platform.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	4	2.7	2.7	2.7
	Yes	146	97.3	97.3	100
	Total	150	100.0	100.0	

The second objective, based on the survey results from Table 3, was achieved through the use of mean score analysis. The mean of the question that the consumer responded that was connected to the dependent variable on a Likert scale from 1 to 5, with the responses being strongly disagree (1), disagree (2), neutral (3), agree (4), and strongly agree (5). The variable that studies the factors that cryptography technology usage has to protect the message system in the online shopping platform is shown in table above as the outcome of mean score analysis.

Perceived usefulness had a mean score of 4.73, perceived ease of use had a mean score value of 4.67, confidentiality had a mean value of 4.73 and lastly, non-repudiation had a mean value of 4.75. Respondents agree that all four factors of cryptography technology usage effect the message system in online shopping platform. Non-repudiation is the factor that related more compare to other factors since it has the highest mean value which was 4.75. According to previous research, female online shoppers who believed that cryptography technology with non-repudiation is favourable to success are more likely to install it sooner in the online shopping platform. Furthermore, according to Redzuan (2016), a system with a non-repudiation factor considers that a user has a favourable relationship between uses and performance. Besides that, Nicole Jonker (2019), another study found that non-repudiation has a mediating function in the relationship between the usage of cryptography technology and message system. Apart from that, there was many articles that identical in content and the outcomes of perceived usefulness, perceived ease of use, confidentiality and non-repudiation are significant since it assists sellers give what the female online shoppers wants.

Table 3
The factors of cryptography technology usage that effect the message system in the online shopping platform.

	N	Mean
PU	150	4.7333
PEOU	150	4.6767
C	150	4.7317
NR	150	4.7511
Valid N (listwise)	150	

H1*:* There is significant relationship between perceived usefulness in cryptography technology to protect the message system in the online shopping platform. According to the findings of coefficient table 4, perceived usefulness had a statistically significant value of 0.000, which

was much lower than the of 0.05. This study's findings revealed a correlation between the independent variables (PU) and the dependent variable securing message system among female online shoppers. Nicole Jonker (2019) stated that perceived usefulness in cryptography technology had a significant effect on securing message system among female online shoppers. By using cryptography technology in areas like online shopping might be a positive development. Furthermore, female online shoppers believed that a system is effective to their success are more likely to have it implemented in their company sooner rather than later. A system with a high perceived usefulness believes that a female online shopper has a positive connection between usage and performance. Since cryptography technology has a factor that could protect message system, cryptography technology and message system have a positive relationship.

H2*:* There is significant relationship between perceived ease of use in cryptography technology to protect the message system in the online shopping platform. Based on the results of coefficient table, it showed the perceived ease of use had 0.000 significant value which the value is lower than 0.05. According to these results, there was a relationship between independent variables, PEOU and dependent variable, securing message system among female online shoppers. Based on Nicole Jonker (2019), the usage of cryptography technology should not need an excessive amount of effort on the part of the consumer. For example, the technology should be simple and easy to understand from the beginning. It should also be noted that the communication system, on which the cryptography technology is based, is a widely spread and utilised technological system. Female online shoppers' perceptions of how simple it is to learn a new technology are relevant in the context of the secure message system. This proved that cryptography technology had perceived ease of use as a factor to protect the message system.

H3*:* There is significant relationship between confidentiality in cryptography technology to protect the message system in the online shopping platform. Based on the results of coefficient table, it showed the confidentiality had 0.037 significant value which the value is lower than 0.05. According to these results, there was a relationship between independent variables, confidentiality and dependent variable, securing message system among female online shoppers. According to Stanford in 2019, in order to protect texts in the message system, cryptography technology is used. Most people use cryptography technology because the messages they're sending are meant to be private. It shows that confidentiality is important in cryptography technology because female online shoppers prefer to use the message system which is confidential. Therefore, it means confidentiality in cryptography technology has a relationship to protect the message system in the online shopping platform.

H4*:* There is a significant relationship between non-repudiation in cryptography technology to protect the message system in the online shopping platform. Based on the results of coefficient table, it showed the non-repudiation had 0.023 significant value which the value is lower than 0.05. According to these results, there was a relationship between independent variables, non-repudiation and dependent variable, securing message system among female online shoppers. As stated by Muhammad Kuliya in 2020, cryptographic non-repudiation is an assurance that an entity cannot claim ownership of a prior undertaking or activity. Female online shoppers preferred to use cryptography technology that has non-repudiation because

electronic messages cannot be denied if non-repudiation is in a system, proving that non-repudiation in cryptography technology has a connection to protect the message system in the online shopping platform.

Table 4
The relationship between the usage of cryptography technology and message system in online shopping platform

Model		Unstandardized B	Coefficient Std. Error	Standard Coefficients Beta	t	Sig.
1	(Constant)	.655	.206		3.186	.002
	PU	.499	.101	.408	4.165	.000
	PEOU	.394	.100	.426	3.953	.000
	C	.378	.180	.358	2.100	.037
	NR	-.327	.143	-.292	-2.292	.023

a. Dependent Variable: DV

Limitations and Future Directions

The study faced several limitations, particularly in data collection, largely due to the COVID-19 pandemic. When the researchers began distributing the questionnaire, the world was under movement restriction orders, urging people to stay at home. Consequently, the researcher relied solely on Google Forms to distribute the survey, which made it challenging to reach the target of 150 respondents. This limitation presented significant challenges, as using only an online platform like Google Forms made it difficult to gather sufficient data during the pandemic's Movement Control Order (MCO).

The study employed non-probability purposive sampling with a sample size of 150 respondents. However, the difficulty in reaching this number through online means alone may have affected the adequacy of the sample in representing the target population. Although the researcher managed to collect data from 150 respondents, the findings might not fully reflect the awareness of cryptography in messaging systems among female online shoppers. Additionally, the respondents came from diverse backgrounds, and some may have struggled with reading and understanding English. The language and sentence structure used in the questionnaire might have been confusing for some participants, leading to poor responses from this minority group. As a result, the data collected could be inaccurate or fall short of the research objectives. While many respondents were aware of cryptography, they were often unable to explain its meaning or provide examples of how it applies in their daily lives. Researchers recommend that future studies explore additional key factors of cryptography beyond perceived usefulness, perceived ease of use, confidentiality, and non-repudiation. Expanding the range of independent variables could provide deeper insights into how cryptography can protect messaging systems and encourage online shopping, especially during periods like the COVID-19 pandemic. Future research should also aim to gather data from all states in Malaysia to enhance the accuracy of demographic studies. Educating female online shoppers about the importance of secure messaging systems and providing them with additional knowledge could improve the relevance of the findings.

Moreover, conducting surveys in person is recommended for future research. The researcher notes that online distribution can make it difficult to verify the accuracy of the sample size. There is a risk that respondents may not thoroughly read the questionnaire and might provide random answers, leading to inaccurate data. To address this issue, researchers could benefit from using a method that allows for direct distribution of survey questionnaires, ensuring the integrity of the sample size. Additionally, future studies could investigate the use of cryptography in companies or businesses, focusing on how employers and employees perceive its effectiveness in safeguarding company data. Research could also identify which cryptographic methods are most suitable for various industries and online shopping platforms. Lastly, incorporating interviews into the survey process is suggested. By interviewing individuals knowledgeable about cryptography, researchers can obtain more detailed and reliable information. This approach would allow for more comprehensive answers to questions related to cryptography, ensuring data is collected from trustworthy sources.

Conclusion

The researcher successfully identified how the use of cryptography technology protects messaging systems among female online shoppers. Data collection focused on female consumers in Peninsular Malaysia who purchase products or services through online shopping platforms. The study aimed to evaluate the impact of cryptography technology on messaging security for these shoppers, providing insights into how secure messaging systems can enhance online shopping experiences. The research, based on surveys and questionnaires, helps understand the protective factors of cryptography technology in safeguarding messaging systems. Businesses need to adapt to the digital landscape and leverage technology to create distinctive and memorable experiences that can foster consumer loyalty. Future research should examine the role of cryptography technology in various companies and businesses, assessing employee and employer beliefs about its effectiveness in protecting data. Studies could explore which cryptography technologies are most suitable for companies and online shopping platforms. Additionally, incorporating interviews with experts on cryptography technology could offer deeper insights into its functionality and effectiveness. Given the current lack of research on cryptography in online shopping platforms, this study contributes theoretically by establishing a foundation for future exploration in this area.

References

Agar, J. (2019). What is technology? Annals of Science, 486-512.

Akhtar, I. (2016). Research Design. Research in Social Science, 68-79.

Banerjee, S., & Kurths, J. (2014). A new dimension in secure communications. The European Physical Journal Special Topics, 1441-1445.

Boyd, J. (2002). In Community We Trust: Online Security Communication at eBay . Journal Of Computer-Mediated Communication.

Buchanan, T., & Whitty, M. (2014). The online dating romance scam: causes and consequences of victimhood. *Psychology, Crime & Law*.

Chen, J. (2014). A Secure End-to-End Mobile Chat Scheme. 2014 Ninth International Conference On Broadband And Wireless Computing, Communication And Applications, 472-477.

Cooksey, R. W. (2020). Descriptive Statistics for Summarising Data. Illustrating Statistical Procedures: Finding Meaning in Quantitative Data, 61-139.

Crane, C. (2021). What Is a Hash Function in Cryptography? A Beginner's Guide. Hashed Out by The SSL Store.

Crossley, J., & Jansen, D. (2021). Saunders' Research Onion: Explained Simply. Grad Coach.

Crossman, A. (2020). What You Need to Understand About Purposive Sampling. ThoughtCo.

Dang, T. (2021). Improving E-Commerce Service For Better. International Business, 5-33.

DeCarlo, M. (2020). Sampling in qualitative research. Pressbooks.

Devi, T. R. (2013). Importance of Cryptography in Network Security. International Conference On Communication Systems and Network Technologies, 462-464.

Dhakal, C. (2018). Interpreting the Basic Outputs (SPSS) of Multiple Linear Regression.International Journal of Science and Research, 1448-1449.

Diggory, K. (2018). Technology in the 21st Century. Explore Life.

Frey, F. (2017). SPSS (Software). International Encyclopedia of Communication Research Methods, 1-2.

Fruhlinger, J. (2020). What is cryptography? How algorithms keep information secret and safe. IDG Communications.

Gencoglu, M. T. (2019). Importance of Cryptography in Information Security. Journal of Computer Engineering, 65-68.

Ginee. (2021). How To Chat Seller In Shopee And How Can I Contact Them.

Huawei. (2021). Quantum computers will disrupt existing systems.

Jones, C. (2010). Utilizing the Technology Acceptance Model to Assess the. Issues in Information Systems, 9-12.

Jonker, N. (2019). What drives the adoption of crypto-payments by online retailers?. Electronic Commerce Research And Applications, Vol. 35, 3-5.

Kartalopoulos, S. V. (2006). A Primer on Cryptography in. IEEE Communications Magazine, vol 44, no. 4, 146-151.

Kasasa. (2021).Boomers,Gen X, GenY, Gen Z, and Gen A explained.

Kuliya, M., & Abubakar, H. (2020). Secured Chatting System Using Cryptography.

International Journal Of Creative Research Thoughts, 23-29.

Lazada. (2021). Help Center.

Lemzy, A. (2018). 9 Types of Mobile Messages to Engage eCommerce Customers. The Branch.

Li, Y. (2016). How to Determine the Validity and Reliability of an Instrument.

Liu, W. (2021). Gold Price Analysis and Prediction based on Pearson Correlation.*Association for Computing Machinery*, 358-361.Market Business News. (2021). Online shopping – Definition and meaning.

McLeod, S.(2018). Questionnaire: Definition,Examples, Design and Types.Simplypsychology.org.

Mishra, P. (2021). 8 Types of Sampling Techniques. Medium.

Miyazaki, A. D., & Fernandez, A. (2001). Consumer Perceptions of Privacy and Security Risks. Journal of Consumer Affairs, 27-35.

Mohsin, M. (2020). 10 Online Shopping Statistics You Need to Know in 2021.

Pedamkar, P. (2021). What is Cryptography? Educba.

Prince, B. and Lovesum, J., (2020). Privacy Enforced Access Control Model for Secured Data Handling in Cloud-Based Pervasive Health Care System. SN Computer Science, 1-3.

Reynolds, L., & Winks, J. (2021). Data Protection Techniques: A Cryptography Approach. Journal Of Technology and Systems, Vol.3, 13-18.

Richards, K. (2020). What is cryptography? TechTarget.

Ross, M. (2018). 5 Ways Messaging is Transforming Customer Service for Online Retailers. Disruptive advertising.

Sardar, Z. (2020). Cryptography: Why Do We Need It? Electronic Design.

Schober, P. (2018). Correlation Coefficients: Appropriate Use and Interpretation. Anesthesia & Analgesia, 1763-1768.

Shashank. (2020). What is Cryptography? – An Introduction to Cryptographic Algorithms. Edureka.

Shopee. (2021). Privacy Policy.

Singh, H. (2021). E-Commerce Security Issues. Cyphere.

Sithamparam, B. (2021). Consumer alert – Scam cases are rising. Free Malaysia Today:

Smart, N. (2018). How cryptography enables online shopping, cloud tech, and the blockchain. TNW Conference.

The Economic Times. (2021). Definition of 'Cryptography'. Varghese, J. (2021). 10 E-commerce Security Threats That Are Getting Stronger By The Day.

Walia, A. (2020). How to formulate a research strategy? Project Guru.

Wong, A., & Yamat, H. (2020). Testing the Validity and Reliability of the “Learn, Pick, Flip”, International Journal Of Academic Research in Business & Social Sciences, 22-26.

Yasin, S., (2012). Cryptography Based E-Commerce Security: A Review. International Journal of Computer Science Issues, Vol. 9, 132-135.

Yin, W. (2021). Top-selling Product Categories that Customers Buy on Shopee - Involve Asia.

Zamlus, N. (2019). Report: Selangor make up highest number of e-commerce users in 2019 - Selangor Journal.

Zou, D. (2020). Using SPSS to Analyze Complex Survey Data: A Primer. Journal of Modern Applied Statistical Methods, 2-6. (Mansor, Zabarani, & al, 2021)